

Perceived Roles of the Internal Auditor in Business Continuity Planning in the  
Government Sector

Dissertation

Submitted to Northcentral University

Graduate Faculty in the School of Business and Technology Management  
In Partial Fulfillment of the  
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

by

MONDAY RUFUS

Prescott Valley, Arizona  
September 2016

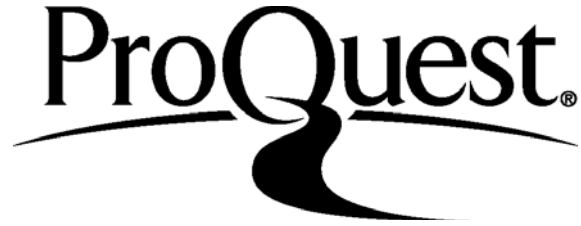
ProQuest Number: 10181966

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest 10181966

Published by ProQuest LLC (2016). Copyright of the Dissertation is held by the Author.

All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code  
Microform Edition © ProQuest LLC.

ProQuest LLC.  
789 East Eisenhower Parkway  
P.O. Box 1346  
Ann Arbor, MI 48106 - 1346

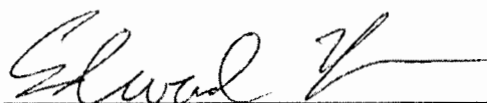
Approval Page

Perceived Roles of the Internal Auditor in Business Continuity Planning in the  
Government Sector

By

MONDAY RUFUS

Approved by:



Chair: Dr. Edward Kim

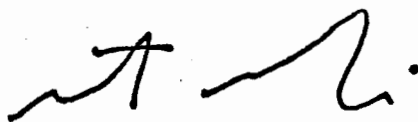
October 12, 2016

Date

Member: Dr. Julia Watkins

Member: Dr. Joseph Oloyede

Certified by:



Dean of School: Dr. Peter Bemski

10/12/16

Date

## Abstract

A government agency is expected to implement a plan to be followed should an emergency arise. This minimizes the impact of disruption and ensures the quick resumption of operations. But without the involvement of those with the right expertise, management of a government agency could assume undesirable business continuity risks. The purpose of this qualitative case study was to understand the perceived roles of the internal auditor in business continuity planning within the government sector. The findings arose from data collected from interviews with individuals using a purposive convenience sample. The data analysis resulted in five themes. The five themes for the overarching research question included: (a) significant negative impact, (b) obstacles, (c) major roles, (d) areas to be excluded from the internal auditor, and (e) internal auditor's independence. Findings from the study indicated that the government sector did not consider risks that could hinder the entity from successful mitigation of disruptions because preference was given to other pressing issues. Other impediments affecting business continuity planning included a lack of adequate communication, resources, periodic testing, staff training, inept personnel, inaccuracy of business impact analysis, and the notion that a disruption would never occur. The Internal auditor's involvement in business continuity planning in the government sector should be in an advisory capacity because of their independence and knowledge of the entity and the risks affecting the organization. To mitigate a threat to the internal auditor's independence and promote objectivity, the organization, and internal auditor should implement safeguards. The implications of this study included providing valuable insights to management, policymakers, and the internal auditor about the perceived roles of the internal auditor in

business continuity planning in the government sector and how to utilize his or her expertise while ensuring independence and objectivity. Three recommendations for future research included: (a) whether the internal auditor should play a role in maintenance and update of the business continuity plan; (b) the reason a governmental sector would be reluctant to test their business continuity plans periodically; and (c) the roles of the internal auditor in business impact analysis during the development of a business continuity plan.

## Acknowledgements

A lot of people were instrumental in my completion of this journey. First, I would like to thank my wife, Ugochi, for your unwavering support throughout the duration of this endeavor. This milestone would not be impossible without your understanding, sacrifice, and support. To my four children, Tina, Jeffrey, Chisom, and Jonathan, I say thank you for all of your support. Even though our vacations plans were affected because of required weekly assignments, you never relented in showing your support. I would also like to extend my hearty thank you to my late mother who always encouraged me to continue to strive for new heights. To my siblings, Ndoma, Chigbundu, Maduabuchi, and Ahuru, I say thank you for your words of encouragement.

Equally important are my associates at the office. You listened whenever I solicited your input during this journey. Additionally, I appreciated your interest in my research topic and periodic inquiries on the progress. I would like to thank the following Northcentral University's faculty members: Dr. Bari Courts, Dr. Mary Beth Klinger, Dr. John Hannon, Dr. Ana Machuca, Dr. Linda Leatherbury, Dr. Alfred Greenfield, Dr. Bob Levsseur, Dr. Anastasis Petrou, Dr. Susan Hebert, Dr. Shakil Akhtar, Dr. J. Dickinson, Dr. Heather Miller, Dr. Kirby Scheer, and Dr. Diane Stottlemyer for your guidance and input. A big thank you goes out to my Chair, Dr. Kim Edwards, and my committee members for this dissertation, Dr. Julia Watkins, and Dr. Joseph Oloyede. I appreciated your timely feedback and encouragement. Finally, my heartfelt thanks go out to the internal auditors in the State of Texas who participated in this study. I sincerely appreciate your time; your input in this study contributed to this significant milestone.

## Table of Contents

Chapter 1: Introduction .....	1
Background .....	3
Statement of the Problem .....	5
Purpose of the Study .....	6
Theoretical Framework .....	7
Research Questions .....	11
Nature of the Study .....	11
Significance of the Study .....	15
Definition of Key Terms .....	16
Summary .....	19
Chapter 2: Literature Review .....	21
Documentation .....	22
How Business Continuity Planning Applies to the Government .....	23
Reasons for Business Continuity Planning .....	26
Internal Audit Function .....	37
Role of Internal Auditor .....	43
The Government and Readiness .....	47
Historical Legislative Perspectives .....	53
Organizations and Business Continuity Planning .....	55
Mitigating a Disaster .....	57
Possible Impact of a Disaster .....	59
Preparing for a Disaster .....	63
Responding to a Disaster .....	65
Summary .....	67
Chapter 3: Research Method .....	69
Research Methods and Design .....	72
Population .....	75
Sample .....	75
Materials/Instruments .....	76
Data Collection, Processing, and Analysis .....	77
Assumptions .....	80
Limitations .....	80
Delimitations .....	81
Ethical Assurances .....	82
Summary .....	84
Chapter 4: Findings .....	86
Results .....	87
Evaluation of Findings .....	102
Summary .....	109

Chapter 5: Implications, Recommendations, and Conclusions .....	113
Implications.....	117
Recommendation .....	124
Conclusions.....	132
References.....	136
Appendices.....	160
Appendix A: Recruitment Letter - Telephone Script.....	161
Appendix B: Recruitment Letter - Email Script .....	162
Appendix C: IRB Approval .....	163
Appendix D: Informed Consent Form .....	164
Appendix E: Interview Guide .....	166
Appendix F: Interview Questions .....	167



## List of Tables

Table 1 Themes for Research Question .....	88
Table 2 Significant negative impact .....	91
Table 3 The obstacles that get in the way of dealing with disruptions successfully .....	94
Table 4 The reason for the internal auditor to play major roles in business continuity planning.....	97
Table 5 The areas the internal auditor should be excluded.....	99
Table 6 Independence of the internal auditor .....	102

## Chapter 1: Introduction

Business Continuity Planning, one of the most common topics in business circles, high-profile meetings, and presentations today, continues to be a major issue, especially in the government sector. More than ever, society expects the government to be genuine and highly reputable, especially when managing disasters or any other crisis (Koronis & Ponis, 2012). The expectation is that this trend will intensify as the political and business environment continues to change considerably. When a crisis is not properly mitigated, there could be a temporary disconnection with the public or other users of services or even permanent disruption of business relations (Koronis & Ponis, 2012). The public expectations have caused some regulatory agency personnel to begin thinking seriously about business continuity planning (Jones, 2011).

For example, in May 2011, a tornado ripped through the City of Joplin, Missouri, and killed 158 people, wounded more than 1,000, and damaged about 8,000 buildings. According to Busch and Givens (2013), government has always emphasized the importance of preparing for disruptions. When a disaster occurs, the purpose of business continuity planning is to ensure critical functions can operate during and after a disaster or other contingency, and then minimize recovery time to reach normal operations (Carrington, 2010). Critical functions may require for the government to include budgetary data, policy and regulatory data, human resource management data, and acquisition and planning data (Office of Management & Budget, 2011). Governments oftentimes worry about continuity as they are under pressure to keep up with the citizens' expectations for optimum services. Additionally, globalization and technological advancements have changed how governments do business (Izumi & Shaw, 2015; Nasim

& Sushil, 2010). For example, since the enactment of the E-government Act by the United States Congress in 2002, government agencies in the United States are steadily taking advantage of e-services. As a result, governments have become more transparent and accountable to the public. Additionally, government services have become more accessible, more efficient, and there is an increased opportunity for the citizens to participate in government. Transactions can be completed online, which may include paying for taxes online, renewing licenses, or even registering to vote. Online presence also provides an opportunity to explore different ways to generating revenue, not only targeting citizens of the United States but also people worldwide (Baird, Zelin, & Booker, 2012). According to Melnik (2015), there has been an increase in the number of cyber-attacks against both United States government agencies and private organizations. For example, cyber-attacks have increased by 35% from 2010 to 2013, specifically, 34,048 to 46,160. A government agency has to create a plan to be followed should an emergency arise (Hall, Skipper, Hazen, & Sawalha, 2012). A well-executed plan minimizes the impact of disruption and ensures the quick resumption of operations. This plan also requires the assessment of risk and the implementation of risk management.

The internal auditor helps the government achieve its objectives of serving the public by evaluating and improving the effectiveness of risk management. The internal auditor reports to the oversight board or a designated committee and is in a position to evaluate management's understanding of risks affecting the organization and the potential impact of any loss (Schneider, Sheikh, & Simione, 2012). The internal auditor also assures the board of directors or its designated committee that management of the organization can effectively mitigate any business continuity risks to acceptable levels

(Stefaniak, Houston, & Cornell, 2012). Additionally, in situations where management has decided to assume the risk of undesirable business continuity risk, the internal auditor notifies the board and also ensures a decision has been adequately documented (García, Barbadillo, & Pérez, 2012).

## **Background**

When a disaster occurs, it affects everyone including the government, businesses, and families. The phrase “business continuity planning” is widely used in business or government. The focus of a business continuity plan is to mitigate potential loss through the identification, prioritization, and safeguarding of critical assets of the business, not just information technology (Hoong & Marthandan, 2014). Good continuity plans include providing an alternative path in support of critical business processes in the event of an emergency, disaster, or other disruption (Carrington, 2010). The roles of the government include protecting its people physically or economically, including, among others, providing welfare, building roads, protecting the border, and funding education. As a result, proper planning is required to ensure mitigation of losses or elimination of the impact of disasters (FEMA, 2015; McGuire & Schneck, 2010). For example, the American Bankers Association and Banking Administrations are expecting their members to implement acceptable business continuity practices to ensure adequate protection of the public interest (Koronis & Ponis, 2012). But historically, governments have not stressed enough about resilience as a required quality for communities. But to stress the importance of preparedness, the federal, state, and local governments have instituted laws, statutes, ordinances, and guidance which may or may not be complied with (Haddow, Bullock, & Coppola, 2011).

The United States government collects taxes from its residents on income generated anywhere in the world (Hickman, 2012). The government sector would rely on business continuity planning to mitigate the impact of any disruption that would affect its ability to collect taxes. The government uses taxes collected to fund these projects (Reid, Waring, Enriquez, & Shivdas, 2012). If the government was unable to process taxes owing to the lack of contingency planning this would be considered an emergency. Preparedness is required to mitigate the effect of disasters affecting the government's system such as tax database (DHS, 2008). Any disruption affecting the government also impacts the public (Shughart, 2011). The management of the government agency would be expected to utilize the right resources, including personnel, to ensure proper implementation of business continuity planning. Implementation of business continuity planning requires an adept knowledge of potential risks and its possible impacts on the government (Glendon, 2013). When proper skills and knowledge are not used to ensure continuity of business, there is the risk of unsuccessful response to a disaster, and potentially significant losses (Kusumasari, Alam, & Siddiqui, 2010; Haque et al., 2012). Although there have been advancements in the government sector in mitigating disruptions, recurring errors continue to exist in the process (DHS, 2011; Faith, Jackson, & Willis, 2011; Oh, 2012; Renaud, 2012). Internal audit as an organizational function thrives on independence. As a result, the internal auditor understands the essence of providing unbiased recommendations to management and those charged with governance or oversight. Although internal auditors are not allowed to participate in decision-making for an entity, owing to their independence, nothing precludes them from providing proactive, risk-based recommendations (Wines, 2012; Zerni, 2012).

## Statement of the Problem

A good plan minimizes the impact of disruption and ensures the quick resumption of operations. But without the involvement of an independent person who understands risk evaluation management of a government agency could assume undesirable business continuity risks. An internal auditor is an independent person who understands risk evaluation. The Auditors report directly to those charged with governance (García et al., 2012). Sufficient literature does not exist on the perceived roles of the government internal auditor in business continuity planning.

Governments are oftentimes ill-prepared to handle disasters owing to a lack of adequate resources, other competing issues, and proper preparation for catastrophic events (Deverell, 2012). Even the *Nationwide Plan Review* conducted by the Department of Homeland Security determined that only 10% of business continuity plans are adequate to mitigate the effect of disasters (DHS, 2006). The lack of adequate preparation could pose a significant challenge to the government should an event occur (DHS, 2011e). Additionally, catastrophic events could result in unnecessary distress, harm, and affect the public's perception of the government (Kusumasari et al., 2010; Shughart, 2011). These shortcomings are usually because of a lack of planning, which may include proper identification of risks, impact analysis, consideration of response alternatives, and testing and maintenance (Coles & Zhuang, 2011; Kusumasari et al., 2010). Consequently, the problem addressed by this study was the lack of the use and the limited understanding of the perceived roles of the internal auditor in business continuity planning in the government sector. Governments oftentimes worry about continuity as they strive to keep up with the citizens' expectations for optimum services. Potential

risks to the government include the loss of mission critical data, displacement of workers, and unavailability of facilities owing to catastrophic events (Gourio, 2012; McEntire, 2012; Raman, Dorasamy, Muthaiyah, Kaliannan, & Muthuveloo, 2011).

### **Purpose of the Study**

This purpose of this qualitative case study was to explore the perceived roles of the internal auditor in business continuity planning within the government sector. Information systems experts and business consultants would agree that it is almost impossible for a government sector to survive when critical systems are unavailable owing to a disaster (Chandra, Williams, & Tang, 2013). In essence, the availability of these critical systems is quintessential in trying to assess a government sector's business risk, which is the likelihood of the ability to achieve its objectives when a disaster strikes. The focus of this case study was internal auditors in the governmental sector from the State of Texas in the United States. Data sources for this study included semi-structured interviews and open-ended questionnaires. To ensure credibility, the people selected were a representative sample of internal auditors affected by the topic under study. Prior to conducting interviews, the first phase of the study comprised using an interview guide (Appendix E) developed by the researcher as a guide to avoid any appearance of incompleteness and inconsistency. The second phase involved sending questionnaires to the internal auditors at various State of Texas agencies. Face-to-face or telephone interviews were conducted with the participants. As fieldwork unfolded, no additional samples were needed due to the depth of discussions with existing interviewees. The individuals interviewed in each participating state agency had the opportunity to respond in their own words to express their personal perspectives about the types and possible

impacts of service disruptions, perceived readiness, and obstacles in dealing with disruptions successfully, and what could help an organization mitigate the effects of service disruptions. The results of this case study could be useful to the State of Texas agencies and internal auditors as they continue to protect the interests of the public. With most processing requiring access to increasingly integrated applications and databases, when the system is down, there is no opportunity to do any meaningful work. The essential nature of information and technology will continue to increase in the future.

### **Theoretical Framework**

The focus of this study was directed toward exploring the roles of the internal auditor in business continuity planning in the government sector. Due to the nature of the identified research problem and purpose, an interpretive approach was determined to be the best theoretical framework. One basic assumption of the interpretive framework is that knowledge is gained or at least filtered through training and oftentimes reinforced by scholarly articles, books, and advisors (Shank, 2006). Additionally, the interpretive framework acknowledges the intimate relationship between the researcher and the topic under study, and the situational constraints that shape the process (Shank, 2006). An interpretive framework, unlike positive, does not predefine dependent and independent variables and is not designed to test hypotheses. Rather, the focus is to produce an understanding of the phenomenon (Shank, 2006). The focus of this study is not to predefine dependent and independent variables or to test hypotheses, but rather to build an understanding related to the perceived roles of the internal auditor in business continuity planning in the government sector.



Interpretation plays a major role in qualitative research. Interpretation involves answering the *why* questions, attaching significance to particular results, explaining findings, and putting patterns into analytical frameworks. To assure correct interpretation, there must be solid description, which is called thick description (Shank, 2006). Correctly conducted qualitative research presents detail, context, emotion, and evokes self-feelings. During interviews, it is easy to interpret incorrectly. For example, a part of business continuity planning is the risk assessment process (Lindell, Prater, & Perry, 2007). During risk assessment, it is easy to misinterpret a threat and probability of impact (Kent, 2011). Also, the lack of pure description and correct interpretation could affect mitigation approaches used by management of the entity including the estimated financial impact (Lindell et al., 2007). Additionally, management of the governmental entity considers different alternatives during the planning stages. Since there is no universal way of planning for mitigation of disaster or disruption, each approach is subject to different interpretations. However, consideration is given to different types of disasters and disruptions and how to mitigate their effects (Haddow et al., 2011).

Another area that is subject to interpretation is the unexpected outcome of an event (Resnick, 1987). An event could be so unique that uncertainty exists as to the approach to be used in responding. Sometimes responders might and would rely on past experiences. But time is of the essence when a disaster occurs; therefore, responders have limited time to develop strategies and no time to assess options (Patterson, Weil, & Patel, 2010). Oftentimes, interpretations of the roles of the internal auditor in business continuity planning might differ because of the background of the researcher, methods used, or objective of the research (Shank, 2006). As a result, objectivity is very

important in qualitative research. One example of thick description utilized in this proposed study was that of *wink*. During interviews, the researcher paid close attention to *wink*, since each description detail presents a different level of interpretation (Shank, 2006). Additionally, the researcher took into account biases and predispositions during both the fieldwork and analysis to get to the true essence of the phenomenon under study (Converse, 2012; Dowling & Cooney, 2012).

The researcher's perspective must be made explicit. Any research strategy ultimately needs credibility to be useful. No credible research strategy advocates biased distortion of data to serve the researcher's personal interests and prejudices (Klein, 2012). In this study, it was important to adopt a stance of neutrality. In addition, it was ill advised to set out to prove a particular perspective or manipulate data to arrive at predisposed "truths."

Although the basic assumption of an interpretive framework lies in the view that there are multiple truths, its approach is more about understanding, which is a primary goal of qualitative research. Such truths could come from culture, belief, media, and false ideologies (Shank, 2006). Such shared belief is considered *intersubjectivity* (Shank, 2006). This study reflected another interpretive framework related to *critical awareness*. The idea was not to show weaknesses only but to outline different ways of making things better. For example, governments implement business continuity plans to ensure mitigation of the effects of any disruptive events, and thereby protect the assets of the public.

In this study, the researcher conducted interviews and identified some weaknesses related to business continuity planning. The participants reflected different ideologies

about the roles of the internal auditor in business continuity planning in the government sector. Such ideologies could be learned or just beliefs (Shank, 2006). Oftentimes, such ideologies could work against a person's or government entity's self-interest (Shank, 2006). For example, a person might believe that the only way to mitigate the impact of service disruptions is through daily back-ups of data, which are kept in the establishment or within close proximity and with the oversight of the internal auditor. However, such ideology could be self-destructive when a disaster occurs. In essence, business continuity planning might encompass much more than securing the entity's data (Klein, 2012).

**Other studies related to the subject under study.** There was a study on the role of the public sector asset manager in responding to climate change (Berenfeld, 2007). The study discussed the need for public asset managers to mitigate and prepare for future events (Warren, 2010). Another study discussed about business continuity management in local governments. It emphasized that disruptions to the services could cause a significant negative impact on the community and could prevent councils from meeting its obligations (Pearson, 2010).

Another study was an assessment exploration of strategic business continuity planning methods in Michigan small businesses (Lasecki, 2009). Another study discussed business continuity management and how to ensure continuity of business by focusing on the critical business processes (Smit, 2005). A study was conducted on the cyclical approach to business continuity planning (Botha & von Solms, 2004). The study discussed the limited business continuity planning by small and medium sized businesses on account of the lack of resources. There was a study on transitioning from business continuity to mission continuity (Mekdeci, 2011). That study focused on protecting

educational technology from potential compromise from a variety of threats including natural disasters, human created risk, and environment dangers.

To recover from any disruption or disaster, a governmental agency needs to design business continuity planning effectively (Allen, 2008). Literature concentrating on the development of a business continuity plan failed to identify the roles of the internal auditor in the identification of critical business processes; risk assessment and defined threats; vulnerability; probability; impact analysis; disaster levels and recovery strategy; implementation; testing; monitoring; and maintenance. Internal auditors of government entities conduct periodic risk assessments and perform audit plans prior to carrying out audit activities. To perform these assessments, they must understand every aspect of the entity and critical nature of each unit. Since business continuity planning also involves conducting an agency-wide risk assessment, it is important to determine the roles of the internal auditor to ensure adequate protection of critical assets of the governmental entity (Dickins & Daughterty, 2012).

### **Research Questions**

Since the purpose of this qualitative single-case study was to understand the use and the perceived roles of the internal auditor in business continuity planning within the government sector, the research question was designed to arrive at this understanding:

**RQ1.** What are the perceived use and the roles of the internal auditor in business continuity planning in the government sector?

### **Nature of the Study**

The focus of business continuity planning is to ensure total survival, especially in the governmental sector. Ineffective implementation and response to a disaster could

pose the risk of significant losses and negative impact on the government and ultimately to the public. When a disaster occurs, the job of the government sector is to ensure its functions can operate during and after a disaster or other contingency, and then minimize recovery time to reach normal operations, and thereby protect the public (Moeller, 2008). To mitigate the risk of substandard business continuity planning the right resources should be utilized. Although no business continuity plan is perfect, the internal auditor, an independent function, understands risk affecting an organization and is in a position to report to management and those charged with governance about issues affecting the organization (McGuire & Schneck, 2010).

This qualitative research focused on understanding the perceived roles of the internal auditor in business continuity planning within the government sector. This case study used purposive sampling to ensure the identification and selection of individuals or groups of individuals with the proper knowledge and experience related to the phenomenon under study. In addition, participants were expected to be available and fully participate in the study. They also were expected to be able to convey experiences or opinions in a coherent manner. The overall objective was to maximize efficiency and ensure optimum validity (Suri, 2011; Patton, 2002; Yin, 2009). Accordingly, Jones (2010) exhibited the same rationale during his research on the leadership of government during an emergency.

Furthermore, the focus of this research strategy is to enhance the consistency and accuracy of the data gathered, by reducing the unpredictability of responses obtained due to the individual understanding of data gathering tools and information (Yin, 2009). Additionally, qualitative research methodology has become increasingly popular within

the field of business continuity research (Rodriguez, Quarantelli, & Dynes, 2007; Stallings, 2007). Also, this research design methodology is widely used within the public policy and administration field. This methodology has been used when a study requires an in-depth understanding of a phenomenon (Haddow et al., 2011). Finally, a host of the significant studies and pertinent findings within the business continuity and crisis management field have used qualitative research methodologies (Munro, 2011).

The primary benefit of employing the qualitative research design methodology was the impartiality in the gathering of data by the researcher by reviewing the pertinent documents first prior to interviewing the participants. This review ensured the elimination of any form of participant bias when responding to the researcher's questions. Additionally, a qualitative case study provided an opportunity to gain a deeper understanding of the subject under study (Munro, 2011).

Data collection consisted of utilizing several sources to ensure adequate understanding of the roles of the internal auditor in business continuity planning in the governmental sector. The first phase included reviewing a sample of business continuity plans for different governmental agencies in the State of Texas to ensure the presence of a business impact analysis, security risk assessment, recovery strategy, implementation testing, and maintenance program, and disaster recovery plan (Dickins & Reisch, 2012; Jarvelainen, 2012). Finally, there were interviews with internal auditors in different governmental agencies in the State of Texas to gain an insight into their perceived roles in business continuity planning within their respective state agencies.

Texas Government Code, Chapter 2102, Section 2102.004 requires that each state agency that has an annual operating budget of \$10 million; or has more than 100

employees; or receives and processes more than \$10 million in cash in a fiscal year establish an internal audit function. A total of 253 state agencies were identified that met this requirement (Texas State Auditor's Office, 2015). Each state agency's internal auditing function was expected to have an internal auditor. Additionally, the internal auditor was required to prepare an internal audit plan by employing risk assessment methodologies that identify individual audits to be performed during each year. Audits included the agency's major system and controls such as accounting systems and controls, administrative systems and controls, and electronic data processing systems and controls (Texas Internal Auditing Act, 2003).

The 80th Texas State Legislature, Senate Bill 908, requires all state agencies and universities to have a business continuity plan or continuity of operations plan under the guidance of the Texas State Office of Risk Management (Texas State Legislature, 2007). The objectives were to ensure a state agency can perform its essential function under all conditions, reducing the loss of life and minimizing property damage and loss, executing a successful order of succession with accompanying authorities in the event of disruption, and ensuring there are facilities from where the agency can perform essential functions, and protecting personnel, facilities, equipment, records, and other assets critical to the performance of essential functions in the event of a disruption.

The essential functions that must continue and restored quickly, as identified by SORM include providing and/or assisting in the provision of basic needs which include water, power, healthcare, communications, transportation services, sanitation services, environment protection, commerce, and financial services. Emergency services include providing and/or assisting local and tribal governments in providing critical emergency

services, including emergency management, police, fire, ambulance, medical, search and rescue, hazmat, shelters, emergency food services, and recovery operations (Texas State Office of Risk Management, 2016)

### **Significance of the Study**

Business continuity planning should ensure the consideration of the potential risks and the probability of occurrence. There must be the identification of critical business processes, risk assessment and definition of threats, determination of vulnerabilities, probability, impact, disaster levels and recovery, implementation and maintenance strategies. In essence, there should be reasonable assurance of sufficient plan to mitigate unwanted risks within certain tolerable limits (Gruiescu, Ioanăș, & Morega, 2010). However, business continuity plans may not consider the necessary attributes required when the proper expertise is not utilized (Erickson, 2006; Henstra, 2010).

The threat of catastrophic events needs to be understood and properly communicated to those charged with the oversight of the government agency as such events could have significant negative effects on the government (Law & Robson, 2014). Service disruptions could jeopardize the government entity's critical products and financial security (Goudsmit, 2012) when the business continuity plan is not planned properly. Recently, there have been instances of disasters that resulted in significant economic losses. Economic losses arising from disasters between 2001 and 2010 approximated over \$1 trillion. This amount doubled the total amount of losses incurred between 1981 and 1990 (Kunreuther & Michel-Kerjan, 2011). As such, management and the oversight body need to rely on an independent function to provide insight into the



nature of risks affecting the government agency, the likelihood of the risks and the risks, and the level of preparedness (Stewart & Subramaniam, 2010).

The internal auditor who is charged with auditing all of the activities should understand the functions of the governmental entity and is in a position to provide independent information regarding risks and the effectiveness of the business continuity plans in a non-cost prohibitive way (Dickey, Schwagel, & White, 2006). Even in the business environment today, internal auditing is considered a significant part of an organization's internal control structure. To reinforce the critical nature of this function, Section 303a of the New York Stock Exchange's Corporate Governance Listing Standards (2013) specifically requires companies to have an internal audit function. Therefore, it is important to ensure management understands internal auditing is an essential part of the organization and is positioned to offer support in risk management (Dickey et al., 2006). The estimated cost of the BP oil spill was \$6.6 billion in the United States and \$1.5 billion in the Caribbean (Kunreuther & Michel-Kerjan, 2011). These uncertainties can be mitigated by properly implementing preventive mechanisms and control processes utilizing the right expertise to address threats and vulnerabilities (Geale, 2012). Also, government agencies are not immune to disasters; therefore, proper business continuity planning is required.

### **Definition of Key Terms**

**Audit committee.** An operating body of the governing body responsible for overseeing financial reporting and providing an ongoing link between the governing body and the independent auditor, separate from management (Gauthier, 2007).

**Business continuity management.** Business continuity management is a process that assures the identification of potential impact of risks that threaten an organization, provide a system for forming resilience and means for an effective and efficient reaction to these threats, and to ensure the eventual preservation and interest of its key stakeholders, reputation, brand and value-creating actions (Calderon, 2003).

**Business continuity risk.** A business continuity risk is a probability that the entity will continue to exist after a significant event (Calderon, 2003).

**Business impact assessment.** A business impact assessment is the evaluation of the entity's requirements based on the importance to business functions (Berenfeld, 2007)

**Business continuity.** Business continuity is designed to allow an organization to examine its processes, so it understands how things work—where the risk points are and how to start establishing mitigation alternatives and approaches (Garcia, 2008).

**Critical business processes.** Processes that must be restored immediately after a disruption of service occurs (Calderon, 2003).

**Disaster.** An event that could result in a loss (Bayrak, 2009).

**Disaster recovery.** Disaster recovery provides for the restoration of critical facilities and IT services such as hardware, software, and telecommunications following a significant event (Bayrak, 2009; Parker, 2011).

**Internal auditing.** Internal auditing has been defined as an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization achieve its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk

management control and governance processes (Burnaby, Hass, & Abdolmohammadi, 2009).

**Independent.** Impartial and unbiased in discharging duties. The internal auditor must have an impartial, unbiased attitude in discharging his or her duties (Sinason, 2011).

**Internal control.** Internal control has been defined as a mechanism implemented by management to assure “the accomplishment of the organization’s objectives” (Tysiac, 2012, p. 24).

**Low impact disaster.** Temporary, little to no damage or loss, easily remedied, may require no organizational response, such as power loss due to thunderstorm or failure to make a backup of data because a key person was out of the office (Bayrak, 2009).

**Major impact disaster.** An event that is long-term, causing destruction or loss of data center, office space, warehouse, or other, such as the first World Trade Center attack in 1993, or a major attack against one or more e-commerce sites such as the February 2000 distributed denial-of-service attack on eBay or Hurricane Sandy of October 2012.

**Medium impact disaster.** An event causing possibly temporary, minor damage or loss that will require some remediation, such as power loss due to an accident that knocked down a pole carrying electric lines, or a computer virus spreading rapidly through the organization (Bayrak, 2009).

**Mitigate.** An action to ensure an occurrence is less severe or harmful (Berenfeld, 2007). Organizations develop and implement business continuity plans to mitigate service disruptions.

**Risk assessment.** Risk Assessment is the quantitative or qualitative determination value of risk associated with specific situations and documented threats (Pinta, 2011).

**Risk mitigation.** Risk mitigation is developing “appropriate, cost-effective controls that work to reduce potential threats or reduce the impact of those threats should they occur” (Mekdeci, 2011).

**Stakeholders.** Individuals, groups, or organizations affected by an organization’s actions, especially whenever there is a disruption of service.

**Threats.** Threats are potential events that could cause technology or facilities to be unavailable or damaged (Mekdeci, 2011).

**Vulnerability.** Susceptible to a risk or harm. As a part of business continuity planning, organizations assess vulnerabilities (Mekdeci, 2011).

## Summary

When a disaster occurs, the purpose of business continuity planning is to ensure critical functions can operate during and after a disaster or other contingency, and then minimize recovery time to reach normal operations (Carrington, 2010). Governments are oftentimes ill-prepared to handle disasters owing to a lack of adequate resources, other competing issues, and proper preparation for catastrophic events (Deverell, 2012). Therefore, they apply their resources toward more critical issues. But government agency has to create a plan to be followed should an emergency arise (Hall, Skipper, Hazen, & Sawalha, 2012). This minimizes the impact of disruption and ensures the quick resumption of operations. A well-executed plan minimizes the impact of disruption and ensures the quick resumption of operations. This plan also requires the assessment of

risk and the implementation of risk management. The internal auditor helps the government achieve its objectives of serving the public by evaluating and improving the effectiveness of risk management. Consequently, the problem to be addressed by this study was the lack of the use and the limited understanding of the perceived roles of the internal auditor in business continuity planning in the government sector. This qualitative research focused on understanding the perceived roles of the internal auditor in business continuity planning within the government sector. This case study used purposive sampling to ensure the identification and selection of individuals or groups of individuals with the proper knowledge and experience related to the phenomenon under study. The researcher used semi-structured interviews and open-ended questionnaires for data collection.

## Chapter 2: Literature Review

This study explored the roles of the internal auditor in business continuity planning within the government sector. When an organization experiences a disruption of service because of a disaster or other unexpected incidents, the responsibility of an organization is to ensure critical functions will continue to operate during or after the incident (Cascardo, 2013). Business continuity plans are the measures an organization has in place to ensure the continuance of business if there is a disruption of normal operation (Lindström, 2012). The primary objective is to ensure mission-critical systems of the entity, such as the government, continue to function at an acceptable level regardless of a disaster or disruption (Randeree, Mahal, & Narwani, 2012). Governments oftentimes worry about continuity as they are under pressure to keep up with the citizens' expectations for optimum services. Additionally, globalization and technological advancements have changed how governments do business (Nasim & Sushil, 2010). A government agency has to create a plan to be followed should an emergency arise (Hall et al., 2012). Thus, an implemented and complete plan minimizes the impact of disruption and ensures the quick resumption of operations.

For example, the United States collects taxes from its residents on income generated anywhere in the world (Hickman, 2012). The government sector would rely on business continuity planning to mitigate the impact of any disruption that would affect its ability to collect taxes. The management of the government agency would be expected to utilize the right resources to ensure proper implementation of the business continuity plan. Implementation of business continuity planning requires an adept knowledge of potential risks and their possible impact on the government (Glendon, 2013). For

example, Malaysia had never experienced tsunami until its occurrence 2006, and because of a lack of proper planning, experience, and expertise, the government was not prepared to mitigate the disruption arising from that event (Raman et al., 2011). Potential risks to the government include the loss of mission critical data, displacement of workers, and unavailability of facilities because of catastrophic events (Gourio, 2012). The internal auditor helps the government achieve its objectives of serving the public by evaluating and improving the effectiveness of risk management. The government internal auditor could assist in risk evaluation during the implementation of business continuity planning. Historically, government internal auditors roles have been in the areas of audit performance, testing the integrity and reliability of the information provided to elected officials or public, participating in measuring performance by reviewing the reasonableness of performance targets and making recommendations to management and elected officials, and assisting elected officials and management in an advisory capacity (Epstein, 2010). Some of the issues affecting governments today are adapting to changes related to information technology (Marsh, Fischer, & Montondon, 2013). But, there has been little or no attention given to the role of the internal auditor in business continuity planning in the government sector. Ironically, information technology is a major part of the business continuity planning (Aikins, 2011).

### **Documentation**

The literature review was conducted by using several online library databases, which included ProQuest ABI/INFORM Global, Roadrunner Search, and EBSCOhost, for peer-reviewed, academic articles with key terms of *business continuity planning*, *internal auditing*, and *government sector*. Different variations of these terms used to

search databases were *disaster recovery, risk management, independent, internal control, mitigation, risk assessment, threats, vulnerability, crisis, and stakeholders*. This document includes 203 peer-reviewed journal articles published within the last five years and properly referenced and cited.

The strategy used to gather appropriate literature included research on information pertinent to business continuity planning and roles of the internal auditor within the government sector in the United States. The literature search involved looking for resources in different journals, books, dissertations, magazines, newspapers conference papers and proceedings, trade journals, and other pertinent journals available in Northcentral University's online database. Each source was reviewed and evaluated to determine its applicability to the subject under study.

### **How Business Continuity Planning Applies to the Government**

Governments serve the public and as such should be concerned about the threats to the continuity of their operations. Just like other organizations, they face different types of risks on a daily basis, which includes failure of established internal controls, catastrophic events, and noncompliance with regulations (Nor Azimah, 2013). Emergency conditions can arise at any time; therefore, it is the expectation of the public that the government protects its assets to ensure continuity of operations. Government leaders need to identify the risks and institute a plan to ensure successful recovery should an event occur (Smith, 2013). As a result, there is a need for the design and implementation of a business continuity plan that provides reasonable assurance of mitigating any emergency (Ditch, 2014).



Although it is almost impossible to predict how long or the severity of a potential disaster, a risk assessment can be used to project the likelihood of a threat such as earthquakes, tornadoes, pandemic, terrorist acts, and other disruptive events (Adini, Laor, Cohen, & Israeli, 2012). A properly conducted risk assessment can also sustain safety, security, and improve the knowledge should an emergency occur; and thereby enhance the resilience of the organizational systems (Johnsen & Veen, 2013). Business continuity planning needs to continue to evolve and expand as it is more than daily backups and facilities for housing staff; it involves the organization as a whole. Even the U.S. Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission identified the need for a business continuity plan and published an interagency paper to the financial services industry. Their goal was to ensure timely response and adequate protection of assets should a catastrophic event occur. The specific objective was to ensure swift recovery and appropriate continuation of critical services following a disaster or any other catastrophic event (Law & Robson, 2014).

The Securities and Exchange Commission firmly believes it is important to have an alternative plan to ensure continuity of operations. As a result, in 2004, the Securities and Exchange Commission enacted rules requiring the National Association of Securities Dealers and New York Stock Exchange members to develop and implement business continuity plans (Law & Robson, 2014). Specifically, the Securities and Exchange Commission requires members of National Association of Securities Dealers and New York Stock Exchange to develop procedures related to major service interruptions. The concept is that among securities professionals this requirement will streamline regulation and ultimately reduce the cost to members (Cereola & Cereola, 2011).

In response to the accounting scandal involving certain high profile organizations, President George Bush signed the Sarbanes-Oxley Act of 2002 (Scott & Nganje, 2011). Additionally, because of recent fraudulent activities in different organizations, management and stakeholders are concerned about the increasing risk related to business continuity (Randeree et al., 2012). For example, corporate fraud has caused the collapse of one of the major auditing organizations (Beets, 2011). Another example was the indictment of Enron's CEO and conviction of other members of management who violated ethics, trust, and integrity tied to the abuse of power (Soltani, 2014). Although Sarbanes-Oxley did not specifically require the implementation of business continuity plans, such provision was indirectly made in the interpretation of Section 404, Management Assessment of Internal Control (Cereola & Cereola, 2011). Sarbanes-Oxley does specifically require member organizations to understand the risks that may have a significant impact on their financial reporting and as a result, business continuity became an integral part of the Sarbanes-Oxley Act (Cereola & Cereola, 2011).

The goal of business continuity planning is not to prevent disasters or service disruptions, but, like an insurance policy, it deals with risk identification and assessment, and planning for the mitigation of losses from an unfavorable incident (Goldberg, 2013). Such planning ensures that an organization will be able to respond to a disaster, and critical business activities will continue to function at an acceptable level (Turulj & Bajgoric, 2012). Business continuity planning could mitigate losses from disasters when properly developed and implemented (Turulj & Bajgoric, 2012). To ensure proper mitigation of losses from disaster, there should be refined methods of understanding

risks, which would involve deploying different expertise in the organization to participate in the risk identification and assessment (Santos, Borges, Canós, & Gomes, 2012).

Business continuity planning and disaster recovery are often used interchangeably, but their objectives are different. Business continuity planning is broader in scope since it encompasses developing, testing, and the continuity of an organization as a whole, including people, facility, and critical information technology (Friedman, 2014). Disaster recovery concentrates on developing, testing, and implementing continuity for critical information technology and business applications (Friedman, 2014). Business continuity planning tends to be utilized to identify the resources, threats, and potential impact of threats, as well as ways of mitigating disruptions affecting the organization as a whole (ISACA, 2012). In essence, to ensure continuity, critical processes of an organization, including IT, need to be restarted or recovered within an acceptable time frame. The lack of awareness and understanding of threats by a segment of the organization could be a hindrance during the formulation of a business continuity plan (Ojha, Gianiodis, & Manuj, 2013). As a result, it is important for senior management, IT managers, and operational employees to get involved in the development of a business continuity plan (Lindström, 2012).

### **Reasons for Business Continuity Planning**

At a minimum, over a billion individuals in different countries worldwide are periodically exposed to disasters and the frequency of disasters is steadily increasing. For example, between 1900 and 1909, about 73 disasters occurred, but during the period of 2000 to 2005, there were instances of 2,788 disasters (Pathirage, Seneviratne, Amaratunga, & Haigh, 2012). According to Chen and Lee (2012), natural disasters occur

about 400 times each year and result in over 70,000 deaths and affect more than 230 million people. These worldwide disasters are affecting different organizations.

Disasters can affect any organization, large or small, and at any level of development (Heller, 2012). In today's dynamic world, organizations are always looking for different ways of achieving their goals and ensure continuity of operations (Spremic, Jakovic, Braje, & Cavlek, 2013). The Internet has steadily been essential to all facets of the world prompting questions on how to manage and govern it (De Turck, Kiriha, & Hong, 2012). Notwithstanding, the past 20 years has seen tremendous advancement toward a technology base that is more universal; therefore, enhancing worldwide connectivity. Additionally, the number of connections and data exchanges has increased (Ghezzi et al., 2013). As more catastrophic events occur, organizations and the public as a whole worry about the continuity of business functions. Additionally, technology has made the world one interconnected marketplace. Organizations are steadily transitioning from stand-alone word processing and paper filing to server-based systems (Friedman, 2014). These systems make it easier to access documents remotely and obtain real-time information. The Internet has steadily become essential to all facets of the world. Businesses are steadily moving to real-time operations; making connectivity very important to ensure achievement of an organizations' objectives (Friedman, 2014).

Advanced technologies are required for mobile computing in the workplace, enterprise resource planning, virtualization, cloud computing, social networking, and faster connectivity to ensure a competitive edge (Nicoll & Owens, 2013). Cloud computing is the method of storing and processing information offsite and it has changed the way business is conducted in the 21st-century (Tudoran & Ionescu, 2014). From an

economic standpoint, cloud computing affords an organization the option of operating without having to pay for hardware, software, maintenance, and data storage costs and management. Cloud computing is also considered to be environmentally friendly because it enhances energy efficiency and has the advantage of scalability (Dudin & Smetanin, 2011). Owing to the continued technological transformations and globalization of computer resources, cloud computing offers organizations many ways of improving productivity; it is estimated that cloud computing has become a \$46 billion business (Aleem & Christopher, 2013). Although cloud computing offers organizations many ways of improving productivity, some are worried about security issues such as hacking (Jeya & Kannan, 2014). Cloud computing is the method of storing and processing information offsite and it has changed the way business is conducted in the 21st century (Nicoll & Owens, 2013). Business continuity plans and critical data stored in the cloud can be easily accessible through laptops, smartphones, and tablets. However, this convenience comes with risks. Internet-based attacks have increased significantly, resulting in severe disruptions in different organizations (Sterbenz et al., 2013). Disruptions can impact recovery time and accessibility of data if business continuity is not properly implemented. However, efficiency is achieved when recovery is accomplished without delay.

The United States has recently had incidents of *denial of service* attacks aimed at different business establishments (Campbell, 2013). These incidents were previously classified as improbable but are currently considered major threats to organizations (Campbell, 2013). Some are considered criminally motivated and could be initiated

internally or externally. As a result, this type of attack should be classified as a business continuity issue.

There is also an increased use of personal data storage devices such as CD, USB sticks, and even smartphones. These devices can be infected, therefore, posing significant risks to organizations. There is also a growing reliance on outsourcing of services to other entities and ergo, and as a result, there are increased security issues related to data as well as reputational risks (Jarvelainen, 2012). As a result, it is important to develop and implement business continuity planning to ensure the protection of critical infrastructure. There are also constant expectations from the public, customers, and government that necessitates building resilient infrastructure to ensure continuity of business functions (Campbell, 2013). To comply with such demands, organizational leaders should adopt the right technology policies as well as procedures and recovery alternatives, and ensure they are tested periodically as a component of the business continuity planning (Heller, 2012). The internal auditor ensures the organization's business continuity incorporates mobile devices that support critical functions and usage of social media. As a result, mobile devices should have scheduled backups, and there should be training on how they are backed up. The internal auditor should also review contracts with mobile device vendors to ensure there is a provision for replacement and it aligns with the recovery time objective.

Over the past four decades, the United States has experienced an increase in losses arising from natural disasters such as wind, hail, tornadoes, and lightning (Goudsmit, 2012). According to the U.S. government's National Climatic Data Center in North Carolina, it is believed that hurricane damage will increase in the future on account

of changes in the atmosphere (Campbell, 2013). Specifically, precipitation will rise as the atmosphere becomes moister; thereby causing more rainfall and flooding. There are also political overtures that may impede mitigating against natural disasters. Some politicians, specifically, the state of North Carolina Republic state legislature, passed in 2012 a law disallowing any plans for flood defense on the potential effects of climate change until 2016 (Campbell, 2013). Although no other states have implemented such a law, it is still important to ensure that critical assets are protected.

Although an organization's leaders can achieve the business' strategic objectives through the utilization of proper technologies, they oftentimes introduce new risks that should be mitigated (Jarvelainen, 2012). Such planning by management provides reasonable assurance of aligning an organization's goals with its business continuity, avoids redundancies, ensures efficiency and effectiveness, and ultimately meets the expectations of the stakeholders (Jarvelainen, 2012). As a result, there is a need for constructing strong and flexible infrastructures and specifying business continuity procedures to ensure restoration of critical business functions within recovery times that are acceptable for an enterprise ("Four emerging", 2012).

Historically, some organizational managers have failed to plan appropriately for disasters because of the lack of ordered priorities or because of the difficulty in determining the potential cost of a service disruption (Malalgoda, Amaratunga, & Haigh, 2013). Sometimes disasters can be predicted in advance. An example was the New Orleans' flooding following Hurricane Katrina. Still, an event shocks many people whenever it occurs. As a result, many government leaders are mandating certain industries to implement and document a business continuity plan that is frequently tested

(Heller, 2012). For example, in the United States, certain industries such as healthcare, utilities, and financial services are required to implement and maintain a business continuity plan. During the World Trade Center attack in 1993, it took Morgan Stanley's employees over 4 hours to vacate the building (Law & Robson, 2014). After that incident, the business continuity plan for the organization had to be revamped to ensure better mitigation of any future events.

More than ever, society expects the government to be genuine and highly reputable, especially when managing disasters or any other crisis (Koronis & Ponis, 2012). The expectation is that this trend will intensify as the political and business environment continues to change considerably. When a crisis is not properly mitigated, there could be a temporary disconnection with the public or other users of services or even permanent disruption of business relations (Koronis & Ponis, 2012). The public expectations have caused some regulatory agency personnel to begin thinking seriously about business continuity planning (Jones, 2011). For example, the American Bankers Association and Banking Administrations are expecting their members to implement acceptable business continuity practices to ensure adequate protection of the public interest (Koronis & Ponis, 2012).

Preparing and implementing a business continuity plan requires different expertise to ensure proper response to events (Davison, 2014). Management of disasters with the right resources, which can include the deployment of the internal auditor for assessing risks, is important (Zaharia, Dragne, & Tilea, 2014). The identification of the right resources might also provide a reasonable assurance of continuity of business after a disaster (Heller, 2012). The internal auditor focuses not only on internal control but



overall organizational risks. This scope ensures the identification of critical business processes; performance of risk assessment and defining threats; determination of vulnerabilities, probabilities, potential impacts, disaster levels and recovery; and implementation strategies. Additionally, reasonable assurance is provided in terms of keeping unwanted risks within certain tolerable limits (Gruiescu et al., 2010).

An organization should have an alternative path in support of critical business processes in the event of an emergency, disaster, or other disruption (Jan & Lurie, 2012). When a disaster occurs, the job of management is to ensure business functions can operate during and after a disaster or other contingency, and minimize recovery time to reach normal operations (Jan & Lurie, 2012). The focus should be to ensure total business survival, not just information technology (Hemond & Benoit, 2012). The ability to recover from an unexpected incident can mean the difference between recovery and loss of the business entirely (Hemond & Benoit, 2012).

Recently, there have been instances of disasters that resulted in significant economic losses. Economic losses arising from disasters between 2001 and 2010 were set at approximately \$1.2 trillion (Kunreuther & Michel-Kerjan, 2011). This amount surpasses the \$528 billion between 1981 and 1990 (Kunreuther & Michel-Kerjan, 2011). For example, the earthquake that struck Japan in 2011 damaged more than 275,000 buildings, 3,559 roads, 77 bridges, and 29 railways and the estimated economic losses were \$210 billion (Farber, 2011). This amount from the Japanese earthquake is approximately double the amount of economic loss from Hurricane Katrina (Farber, 2011).

The tsunami disaster shows how modern societies' interdependencies make them susceptible to disasters as damage to networks could affect the delivery of key services (Farber, 2011). Also, the McLure fire of 2003 was the worst fire in British Columbia in terms of damages caused and as a result, many businesses incurred significant economic losses totaling approximately \$5.6 billion (Cox & Perry, 2011). Owing to the fire loss, approximately 200 top businesses decided to close their businesses permanently (Cox & Perry, 2011). The government, just like other organizations, could be affected significantly by disasters without notice (De Smit, Lagadec, & Leysen, 2012).

The SARS infection epidemic that occurred between 1996 and 2006 comprised over 3,000 cases and more than 1,300 deaths (K. Lee, Lan, Wang, Fang, & Shiao, 2014). Those incidents resulted in a significant customer decline in Chinese eateries in North America. As a result, some scheduled conventions were canceled, which ultimately affected several cities and necessitated the intervention of the government (K. Lee et al., 2014). The terrorist attack that occurred in the London, England in 2005 caused 55 deaths (Ramiah & Graham, 2013). That attack significantly affected the country's transportation and telecommunications systems.

Another example of instances of disaster with significant business impact was the BP Deepwater Horizon spill that occurred in 2010 (Farber, 2011). BP personnel spent about 3 months trying to stop the flow of oil. Additionally, Hurricane Irene in 2011 caused a significant economic loss due to flooding in the northeast (Farber, 2011). The estimated cost was \$6.6 billion in the United States and \$1.5 billion in the Caribbean (Kunreuther & Michel-Kerjan, 2011). An organization's leaders can mitigate this type of uncertainty by implementing preventive mechanisms and control processes to address

threats and vulnerabilities (Geale, 2012). Also, government agencies are not immune to disasters; therefore, proper business continuity planning is required. Such planning would necessitate gathering the right internal and external resources and properly deploying them to ensure prevention or mitigation of disasters (Geale, 2012).

Oftentimes senior management and the majority of the members of an entity lack the awareness and an adequate understanding of the business continuity process (Niemimaa & Jarvelainen, 2013). These entities include the government, financial institutions, utilities, and healthcare (Lindström, 2012). As a result of this lack of awareness and understanding, there is the reluctance to implement a business continuity plan, and this lack of knowledge could determine whether an entity continues to exist (Malalgoda et al., 2013).

There were studies in various areas within business continuity planning. These included the need for public asset managers to mitigate and prepare for future business continuity planning management in local governments, an exploration on business continuity planning in Michigan small businesses, how to ensure continuity of business in general small and medium businesses, and on education technology (Botha & von Solms, 2004; Lasecki, 2009; Mekdeci, 2011; Smit, 2005; Warren, 2010). But none of the studies addressed the roles of the internal auditor in business continuity planning in the government sector. To recover from any disruption or disaster, government agencies need effectively designed business continuity plans (Lindström, 2012).

Management and audit committees need to rely on an independent function such as the internal auditor to provide information regarding the nature of risks, the likelihood of the risks, the significance of the risks, and conditions of the organization's

preparedness (Stewart & Subramaniam, 2010). The internal auditor is charged with auditing all of the activities of an organization and understands the organization and is in a position to provide assurance to management that the business continuity plan is effective, key personnel are knowledgeable of the business continuity plan, its execution is practical, and that it is cost-effective (Dickey et al., 2006). In the business environment today, internal auditing is considered a significant part of an organization's internal control structure. To reinforce the critical nature of this function, Section 303a of the New York Stock Exchange's Corporate Governance Listing Standards (2013) specifically requires companies to have an internal audit function. Therefore, it is important to ensure management understands internal auditing is an essential part of the organization and is positioned to offer support in risk management (Dickey et al., 2006).

No entity is immune to the threat of service disruptions. Service disruptions could jeopardize an entity's critical products and financial security (Goudsmit, 2012).

Although developing and implementing a business continuity plan involves a significant financial commitment, the cost of not developing and implementing one could be greater. An example is the earthquake in Japan that cut off critical pharmaceutical equipment of the biotechnology company that had facilities in the United States. The high wind from the earthquake caused significant property damage and disruption of services. A part of the business continuity plan is the purchase of adequate insurance protection (Goudsmit, 2012).

Business continuity planning involves more than just a plan for information systems. The first step to be considered in business continuity planning is the business impact analysis which identifies risks and reveals the financial, human, and reputational

impact on the organization (Lindström, 2012; Nicoll & Owens, 2013)). There are different approaches for performing a business impact analysis. One is the use of a questionnaire which is circulated to the appropriate individuals in the organization. The information is obtained, tabulated, and analyzed (Ojha & Gokhale, 2009). The next step is developing recovery strategies. These are a combination of preventative, detective and corrective measures. A primary goal would be to develop a strategy that identifies the best way to recover critical systems in case of interruption. The appropriate strategy would be the one with a cost for an acceptable recovery time that is also reasonable compared to the impact and likelihood of occurrence as determined in the business impact analysis (Goudsmit, 2012; Jarvelainen, 2012).

The next step in business continuity planning involves developing a plan. Based on the input received from business impact analysis and the recovery strategy chosen by management, a detailed business continuity plan is developed (Lindström, 2012; Randeree et al., 2012). The various factors usually considered include pre-disaster readiness covering incidence response management to address all incidences affecting the organization, evacuation procedures, procedures for declaring a disaster, procedures for declaring a disaster, the clear identification of the responsibilities in the plan, and the identification of the various resources required for recovery and continued operation of the organization (Jarvelainen, 2012; Sawalha, Anchor, & Meaton, 2012).

The next step in the business continuity planning involves testing the business continuity plan to determine how well the plan works. The test should address all critical components and simulate actual primetime processing conditions. There should be training and exercises to ensure awareness of respective responsibilities. Additionally,

there should be detailed documentation of observations, problems, and resolutions. This documentation serves as important historical information that can facilitate actual recovery during a real disaster. Business continuity plans should be reviewed and updated on a scheduled basis to reflect continuing recognition of changing requirements (Bajgoric, 2014; Randeree et al., 2012).

### **Internal Audit Function**

An internal audit is an independent function within an organization that is responsible for evaluating the effectiveness of enterprise risk management control (Burnaby et al., 2009). Stewart and Subramaniam (2010) examined the independence and objectivity of the internal auditor by reviewing the reporting relationship of the internal auditor within an organization and the roles the internal auditor plays in assurance, consulting activities, and risk management. Internal auditors were found to play an important role in strengthening risk assessment and internal control (Stewart & Subramaniam, 2010). Additionally, Christopher, Sarens, and Leung (2009) discussed the importance of the internal auditing function in enhancing corporate governance. The enactment of the Sarbanes-Oxley Act has made it even more essential for business managements to rely on the internal auditor during a review of internal control. Internal auditors provide additional services, which are usually initiated by the board of directors or audit committee and management to ensure proper accountability (Christopher et al., 2009).

Internal auditors assume advising responsibilities to ensure the improvement of an organization's fundamental process (Badara & Saidin, 2013). They must propose an audit plan based on risk assessment. Additionally, they help an organization maintain

appropriate internal control. Internal auditors are involved in continuous risk assessment and evaluation to ensure the achievement of organizational goals (Burnaby & Hass, 2011).

The internal control provides reassurance to the users of the reliability of information presented to the stakeholders (Lenz & Sarens, 2012). The public wants to be sure the government sector is run very efficiently and effectively. Additionally, external auditors expect organizations to have a good internal control (Lehman, 2010). The internal auditors are usually very knowledgeable about the activities of the organization and could add value during the development and implementation of a business continuity plan to provide reasonable assurance to the public about the objectivity of the information presented (Sinason, 2011).

**Internal audit and independence.** For an internal audit to be effective it must be independent (Al-Matari, Al-Swidi, & Fadzil, 2014). In essence, the work of the internal auditor should be free from the influence of the management of an organization. Internal auditors, especially the heads of the internal audit functions in organizations, usually have certifications in any of the following: Certified Public Accountant granted by a state board of public accountancy under standards promulgated by the American Institute of Certified Public Accountants, Certified Internal Auditor granted by the Institute of Internal Auditors, or Certified Information Systems Auditor granted by the Information Systems Audit and Control Association (ISACA). Each of these professional bodies has different standards with which their licensees must comply. Some of these standards include undergoing periodic external quality control reviews and maintaining minimum continuing education credits (Al-Matari et al., 2014). Continuing education allows them

to be proficient in different areas including the identification of fraud risks, threats to business continuity, risk assessment, IT skills, and conducting business impact analysis (Dickins & Reisch, 2012).

**Internal audit and risk management.** Internal auditors are required to comply with the Institute of Internal Auditor's International Standards for the Practice of Internal Auditing (de Zwaan, Stewart, & Subramaniam, 2011). In 1999, the Institute of Internal Auditors redefined internal audit to encompass three areas: (a) risk management, (b) control, and (c) governance (de Zwaan et al., 2011). Enterprise risk management has been defined as a process which is effected by those charged with governance within an organization, management, and other applicable personnel assigned to identify potential threats or events that could potentially affect an organization, manage the risk to an acceptable appetite, and provide reasonable assurance of achieving overall objectives of the organization's goals and objectives (Hosban & Hamdan, 2015; Pang & Li, 2013).

Internal auditing is a significant component of an entity's governance, overall risk management, and internal control (Anderson, Christ, Johnstone, & Rittenberg, 2012). The internal auditor provides an independent evaluation of systems in place within an organization and provides reasonable assurance to the management on whether internal control is functioning as intended (Guxholli, Karapici, & Gjinopulli, 2012). Management has to institute a good internal control to ensure proper documentation and implementation of the business continuity planning (Jalba, 2013). In the past, internal auditors analyzed documents, reconciled bank accounts, identified issues, and made recommendations for eradicating the cause of the issues discovered (de Zwaan et al., 2011). More of the issues identified related to errors made by staff or the lack of



understanding of established policies and procedures (de Zwaan et al., 2011). Owing to the increased reliance on technology and the number of vulnerabilities and threats, an organization could leverage the knowledge of the internal auditor during the development of the policies and procedures related to business continuity to ensure alignment with the overall organizational risk management and reduce redundancies (Mekdeci, 2011). A good business continuity strategy is to conduct a periodic business impact analysis on the critical systems to make sure they are still valid (Jarvelainen, 2012). The business impact analysis serves as an introduction to the issues facing the government in terms of resources, critical systems, and operations. The government sector can use the business impact analysis to evaluate threats and risks and critical systems required to provide services. Based on the business impact analysis, the government, just like other organizations, can determine the recovery time objective for critical functions. The recovery time objective is the maximum time allowed to recover a business unit or function. If the recovery time objective is surpassed, the government sector will incur a significant loss. An organization may use a combination of questionnaires and interviews during the business impact analysis. The internal auditor is in a position to facilitate the development of the questionnaires to ensure they are sufficient and relevant (Stewart, 2009).

The management of a government sector might sometimes be worried about regulatory mandates and privacy issues such as health and human services, whether information technology strategies are aligned with the overall organizational goals and regulatory requirements fulfilled (Ayalon, 2011). Additionally, the oversight board wants to ensure that appropriate controls are considered to provide reasonable assurance

that data integrity is guaranteed in the event of a disaster (Odoyo, Omwono, & Okinyi, 2014).

Additionally, the internal auditor could serve as a resource during the update of the business continuity plan to ensure significant changes to critical business processes have been captured (Mekdeci, 2011). A good business practice ensures that backups are frequently tested to confirm that data can be restored to form in the event of a disaster and that restoration can occur within the recovery time objective and recovery point objective instituted by an organization (Sawalha, Anchor, & Meaton, 2012). The internal audit reviews the business continuity planning to ensure that there is periodic training and awareness regarding threats and vulnerabilities (Camara, Crossler, Midha, & Wallace, 2011; DHS, 2015).

Another role of the internal auditor would be to make sure that during the procurement process of third party providers, a full cost and benefit analysis was performed to ensure that the outsourcing made sense and proper diligence was sufficiently performed (Kent, 2011). The analysis might include determining whether it would be cheaper to perform the process in-house in lieu of outsourcing (Kent, 2011). In essence, if the data center were operated in-house, how much would it cost the organization versus outsourcing the function; this might include getting the key business units to be involved in the process (Nicoll & Owens, 2013). This process is considered a transfer of risk to another entity; however, it is a part of the organization's cost in the business continuity planning process (Wees, 2013). An organization's objective should be to ensure that the cost of the business continuity planning does not outweigh its benefits (Baker, 2012).

To further support this assertion of the independence of the internal auditor, Franck and Sundgren (2012) found organizations that have internal audit functions are more likely to discover and report fraudulent activities than those operating without any. Marques (2014) added that internal auditors are likely to uncover fraudulent activities and corruption. As a result, an organization can expect the internal auditor to assess objectively the threats and risk factors affecting the entity to ensure continuity of business processes if a catastrophic event occurs (Franck & Sundgren, 2012). A conflict might arise on account of a simple disagreement between individuals, groups, and departments in organizations, such as the government, in determining critical businesses or allocating the resources earmarked for business continuity business. Since no organization is immune from conflicts, the internal auditor is in a position to serve as the eye of the board of directors in making sure the overall interests of the organization is represented, especially, when analyzing the need for a business continuity plan. A conflict that is not adequately or independently resolved, especially when related to business continuity planning, could negatively affect an organization (Mukhtar, 2013).

Owing to regulatory requirements, there has been an increased awareness and demand for internal assurance within organizations (Dickey et al., 2006). Internal assurance includes the need for adequate internal control and risk management. Independence and objectivity are required to accomplish this task, and the internal auditor is in a position to provide this assurance (Soh & Martinov-Bennie, 2011). The Health Insurance Portability and Accountability Act and the Sarbanes-Oxley Act are examples of the increased regulations that warrant the need for the protection of organizations' assets. Furthermore, there has been an increase of dangers related to

terrorism, natural disasters, and even fraudulent acts within organizations (Randeree et al., 2012). These threats pose significant risks to organizations, especially governmental agencies whose services are needed at all times. Also, the media exaggeration has amplified the public perception of these risks (Randeree et al., 2012).

### **Role of Internal Auditor**

Generally, the internal auditor would make a recommendation for the improvement of the processes in place. Management valued the opinion of the internal auditor, and as a result relied immensely on that function. Nowadays, internal auditing has expanded to encompass functioning in an advisory capacity to management and those charged with governance (de Zwaan et al., 2011). Additionally, the internal auditor is charged with addressing concerns about risk identification, risk evaluation, and the implementation of internal control to ensure achievement of an organization's goals. As a result, many organizations have begun paying more attention to internal auditing and enterprise risk management structures (Jalba, 2013).

Although organizations may be aware of the need to protect their assets, some are not knowledgeable or are reluctant to implement a business continuity plan (Pathirage et al., 2012). Therefore, involving the internal auditor ensures that these critical business processes are identified. If any are excluded by management, possibly on account of unnecessary conflicts, the unbiased internal auditor is in a position to report such omission to the board of directors (Randeree et al., 2012). The internal auditor is in a position to relay to the board of directors or its designated committee whether management understands risks affecting the organization and the potential impact of any loss (Schneider et al., 2012). The internal auditor also assures the board of directors or its

designated committee that management of the organization can effectively mitigate any business continuity risks to acceptable levels (Stefaniak et al., 2012). Additionally, in situations where management has decided to assume the risk of undesirable business continuity risk, the internal auditor notifies the board and also ensures sure a decision has been adequately documented (García et al., 2012).

The internal auditor evaluates critical functions within the organization and as such participates in the improvement of governance, risk management, and control processes (Christopher et al., 2009). Internal auditors are expected to promote the right ethical values by communicating significant risk exposures to the appropriate level of management and those charged with governance (Leung, Cooper, & Perera, 2011). As the evaluators of critical functions, the internal auditors understand the need for business continuity planning (Christopher et al., 2009). Additionally, due to their knowledge of the organization and understanding of risk management, they understand firsthand the steps that should be taken to ensure proper development and implementation of business continuity planning (Christopher et al., 2009). They can also educate management and those charged with governance on potential threats to the organization, and the importance of supporting business continuity planning with adequate resources (Kanellou & Spathis, 2011). Resources include the right individuals and funds needed for the business continuity plan. The internal auditors can also assist in educating employees and creating proper awareness and ensure activities align with overall objectives of the organization (Kanellou & Spathis, 2011).

Internal auditors determine whether the structures implemented by management are adequate and functioning appropriately (Jalba, 2013). In essence, internal auditors

can change management's strategic objectives through recommendations based on the execution of the internal audit plan. Management values the work of the internal auditors not only because of their independence but because of the standards they follow in accomplishing internal audit tasks (Soh & Martinov-Bennie, 2011). The work of the internal auditor requires collecting data and evaluating risk; this aids in providing pertinent information in an advisory role. The roles are advisory in matters related to information technology systems and strategic risks affecting the organization (Leung et al., 2011). Additionally, this function is considered a first-line of defense in opposition to unacceptable response to corporate risks (Muqattash, 2011). The internal auditor's role is explicitly specified by those charged with governance or its designated audit committee (Muqattash, 2011).

**Authority of the internal auditor.** The internal auditor, who is the head of the internal audit function, provides an objective assessment of risk management and reports to those charged with governance within an organization. Those charged with governance is the board of directors of an organization or its designated committee (Dickins & Daughterty, 2012). The authority of the internal auditor is documented in the organization's internal audit charter, which is approved by those charged with governance or its designated committee (Holt, 2012).

The authority of the charter helps ensure objectivity by the internal auditor (Aikins, 2012). For example, a government agency manager cannot try to reduce the scope of the internal auditor's function or even reject the recommendations of the internal auditor without the approval of the board of directors. In essence, the management of an organization cannot override the mandate of a charter without the approval of the board

of directors (Aikins, 2012). As a result, the internal auditor is believed to be impartial and unbiased in the discharge of his or her duties (Muqattash, 2011).

The Institute of Internal Auditors requires that the internal auditor maintain objectivity and be independent in performing his or her duties (Muqattash, 2011).

Internal auditors in the government sector are considered watchdogs because they are in a position to promote trust and accountability owing to their independence (Elmore, 2013).

As a result, the internal auditor avoids any conflicts of interest and is free to report any corporate risks and serve as an early warning system to the board of directors and the organization as a whole. For example, a part of developing a business continuity plan is identifying critical business processes to ensure adequate protection and recovery (Randeree et al., 2012).

**Internal auditor and third parties.** The participation of the internal auditor ensures full knowledge of the contract terms between the organization and the third-party providers (Nicoll & Owens, 2013). This knowledge provides an opportunity for the internal auditor to monitor the contract requirements and risks associated with the third parties. Some of this monitoring might include reviewing for compliance with business continuity, adherence to laws and regulations, or maintenance of certain financial ratios or other key performance measures to continue to qualify to contract with the government agency (Nicoll & Owens, 2013). Another key role of the internal auditor would be to determine how data will be transmitted, received, and validated, and whether a third party is to be used for back-up of data (Wayman, 2013).

The internal auditor could facilitate the testing of application controls of the third party (Wayman, 2013). During that process, the internal auditor might discover certain

application controls are different for providers being considered, even though the data field layout might be the same. Additionally, the internal auditor would ensure the third party has sufficient information security policies, guidelines, and monitoring. The agreement with the third party could include a requirement to encrypt all data files and maintain them on a secure network (Wayman, 2013).

The internal auditor would also review the third party's business continuity to ensure there is a procedure for recovering critical data (Wayman, 2013). Alternatively, the internal auditor might determine whether the third party service provider has undergone an external review performed in accordance with the American Institute of Certified Public Accountants on Standards for Attestation Engagements No. 16, previously known as No. 70. This could limit the level of front-end information technology review to be conducted by the internal auditor (Wayman, 2013).

The members of management and those involved in the activities of the organization might not be cognizant of the internal control and its effect regarding the third party (Wayman, 2013). They also might not know the role of the internal auditor in helping the organization mitigate risks. To help ease this issue, the internal auditor might conduct training sessions in internal controls, the roles of the internal auditor within the organization, and risks associated with third party service providers (Wayman, 2013).

### **The Government and Readiness**

A study indicated that management of public sector organizations spend relatively more time than their private counterparts dealing with different crises (Thach, 2012). One explanation is because they are responsible to various constituencies and changes related to legislation and budget (Thach, 2012). Any significant service disruption within



a government agency affects its stakeholders, including the public (Leverty, 2012). As a result, government agencies must be readily available to ensure the protection of the public during disasters. Prevention cannot be accomplished without a steady or periodic assessment of risks (Chang, Huang, Roan, Chang, & Ying, 2014).

**Types of disasters.** Organizations and communities are steadily exposed to different types of disasters warranting the need for business continuity planning (Afedzie & McEntire, 2010). The different types of disasters that can affect the government may include inherent, environmental, external, and internal disasters. Inherent disasters may include fire, flood, and tornado; environmental disasters may include power outages or no telephone; external disasters may include terrorism and sabotage; and internal disasters may include employee misdeed, fraud, and accident (Bajgoric, 2014; Verchick & Hall, 2011). Government agencies, just like other organizations, must develop a business continuity plan using different relevant expertise to ensure proper identification of risks, threats, impact analysis, and mitigations of those of risks (Afedzie & McEntire, 2010).

Inherent disasters can occur at any time, and when it happens, it can affect an entire region, city, state, and even international boundaries. As a result, organizations, such as government entities, need to plan for unforeseen events by deploying the relevant resources to ensure adequate mitigation of potential disasters (Amancei, 2011). For example, the state of Iowa has experienced three catastrophic floods since 1993 (Verchick & Hall, 2011). The 2008 floods significantly affected cities within Cedar Rapids and other neighboring communities and caused several million dollars in property damages (Verchick & Hall, 2011).

Uncertainties created by inherent disasters have caused experts in the United States to begin paying significant attention to rainstorms (Maurice, 2013). Maurice (2013) felt the frequency and intensity of rains are to be blamed for the precipitation increase noticed in the United States over the last half-century. Heavier rains, floods, and hurricanes increase the chances of larger property damage. For example, it is estimated that the flooding that occurred in the United Kingdom in 2007 affected about 7,000 organizations and caused over \$4.5 billion in damages (Wedawatta & Ingirige, 2012). Other inherent disasters include heat waves, wildfires, and even epidemic illnesses, which ultimately may affect the continuity of critical operations of the government (Verchick & Hall, 2011). These potential disasters could significantly disrupt services and cause a delay in restoring critical governmental functions and negative reactions from the public may ensue (Lester & Persia, 2011). Well-designed business continuity planning would include identification of these threats, their probability of occurring, and indicate an objective plan for the mitigation of any possible service disruption (Gunnec & Salman, 2011). However, these tasks would require the expertise of those with risk management experience, such as the internal auditor (Anderson et al., 2012).

Cities in the United States face disaster risks. However, some have the highest natural disaster exposure risks, such as Miami, New Orleans, Oakland, San Francisco, Honolulu, San Jose, Houston, Los Angeles, and Long Beach (Sun, 2011). Also, many interior cities, such as Oklahoma City, Tulsa, Sacramento, and Memphis face serious disaster risks (Sun, 2011). In 2008, there were 37 natural catastrophes, which resulted in about \$25 billion in losses (Born & Klimaszewski-Blettner, 2013). Government agencies in the United States can easily be affected by any of these catastrophic events. As a

result, proper business continuity planning is required to ensure mitigation of disruptions that may be caused by these events (Omar, Alijani, & Mason, 2011).

The terrorist attack on the homeland of the United States on February 26, 1993, left an indelible mark on the history of the United States (Sorial, 2011). Prior to this incident, terrorism was considered an external issue with a remote or no potential impact on the United States (Sorial, 2011). On that date, Islamic terrorists ignited a 1,500-pound bomb in the World Trade Center that killed six people and critically injured hundreds of people (Law & Robson, 2014). Many thought that was an aberration because the stock market was not hugely impacted; the next day the market fall was less than 1% (Law & Robson, 2014).

The year after the 1993 World Trade Center bombing, the stock market experienced an average gain of 13.7% (Law & Robson, 2014). That event was quickly forgotten until September 11, 2001, when the United States was hit again. On that day, two planes crashed into the World Trade Center; one crashed into the Pentagon, and another into a field in Pennsylvania. Those events have permanently changed the United States as a nation (Sorial, 2011). As a result, there were an estimated 2,700 deaths reported in New York and 125 in the Pentagon, and an economic loss of over \$80 billion (Sorial, 2011).

Many organizations had not been adequately prepared to mitigate the impact of those World Trade Center attacks (Law & Robson, 2014). Although overall, disaster recovery and business continuity planning were in place; they were not adequately implemented (Law & Robson, 2014). As a result, many organizations were not able to continue providing services after the September 11, 2011, attacks and eventually

discontinued business operations (Law & Robson, 2014). On August 14, 2003, New York City experienced an electrical blackout that is still considered one of the largest catastrophic events in United States history (Farley & Weisfuse, 2011). The blackout, which lasted approximately three days, affected eight United States' cities and parts of Canada.

The threats of catastrophic events need to be understood as such events could have significant negative effects on the government (Law & Robson, 2014). Lessons learned from different catastrophic events are that unexpected events may have a negative impact on an establishment if there are no strategies for mitigation (Grimaila & Badiru, 2013). Some establishments fail to recover from a disaster because of insufficient knowledge of threats, vulnerabilities, and the lack of resources (Chang, Wilkinson, Potangaroa, & Seville, 2012). Some establishments fail to recover from a disaster because of insufficient knowledge of threats and vulnerabilities (Malalgoda et al., 2013). Additionally, there might be the lack of specified responsibilities and coordination, and the use of inappropriate expertise during the development of the business continuity plan (Malalgoda et al., 2013). To ensure adequate readiness, business continuity planning would require the deployment of different expertise, such as the internal auditor, to participate in business impact analysis, risk assessment, and designing the right solution for the establishment (Pierson, 2013).

A large percentage of entities fail to understand how business continuity planning could mitigate the impact of service disruptions, including the different roles involved in its implementation (Chamlee-Wright, 2010). Business continuity planning, a risk management process, should be in place and properly implemented by the government to

ensure mitigation of disasters and protection of consumer interest (Lindberg & Seifert, 2011). For example, insurance companies, as well as other segments of the financial services industry, should make sure that risk management programs are in place and functioning properly (Karim, 2011). The companies must be monitored by state regulatory agencies as required by law to ensure adequate protection of consumer interest (Lindberg & Seifert, 2011). Ironically, governmental entities sometimes do not have the right information or tools to make decisions (Ben-Shahar & Logue, 2013). Additionally, they have limited resources to monitor those they regulate (Ben-Shahar & Logue, 2013).

The United States has faced its share of disasters and as a result, there have been efforts by the government sectors, including nonprofits, healthcare, and academics, to prepare for and mitigate disasters (Staley, Zelman, Porto, Hobbs, & Paul, 2009). When a disaster occurs, the job of the governmental agencies is to ensure their functions can operate during and after a disaster or other contingency, and then minimize recovery time to reach normal operations, thereby protecting the public (Johnston, Becker, & Paton, 2012). As a result, there must be an alternative path in support of critical business processes in the event of an emergency, disaster, or disruption of services, which would include establishing goals. These goals must be supported by management and those charged with governance as well as incorporated into the overall management of the organization (Karim, 2011). There must be an agency-wide risk assessment that would include the identification of threats, the probability of occurrence, and business impact analysis (Pinta, 2011). There must be strategies for mitigating the impact of service disruptions, a business continuity plan development, implementation, training, testing, and periodic reviews (Nicoll & Owens, 2013). A governmental agency could lack the

expertise to carry out these tasks; therefore, the internal auditor could serve as a facilitator in this effort (Pierson, 2013).

The internal auditor should be in a position to provide assurance to management and those charged with governance that response plans related to the business continuity plans are appropriate, flexible, and adaptive and that the individuals identified in the business continuity plans are capable of executing the recovery process effectively. Additionally, the internal auditor could ascertain that the business continuity plan is regularly reviewed and that it is updated when deemed necessary, especially when new threats and vulnerabilities are highly probable (Mix, 2012).

### **Historical Legislative Perspectives**

No entity is immune to disasters. In 1973, the United States enacted the Flood Disaster Protection Act by expanding national flood insurance (Herbane, 2010). In 1977, the US Foreign Corrupt Practices Act was enacted (Herbane, 2010). Although the US Foreign Corrupt Practices Act was enacted to thwart and indict cases of bribery and corruption of foreign officials, it also included a provision requiring the keeping and safeguarding of organizational records from damage (Darrouh, 2010). These new accounting rules were enacted to provide reasonable assurance of preventing, among other things, unlawful or unsupported transactions and misrepresentation of data or records (Weber & Wasieleski, 2013). Additionally, these rules would provide the possible benefits of improved financial reporting and compliance with applicable laws and regulations (Krishnan & Yu, 2012). To ensure compliance with these rules, insurance companies must be steadily monitored by insurance regulatory agencies (Karim, 2011). Such monitoring would require the availability of data whenever needed

(Karim, 2011). Additionally, management needs timely information to ensure proper assessment of operational risks (Năstase & Unchiașu, 2013). As a result, governmental agencies would benefit from well-designed and implemented business continuity planning. Such timely information would afford management an opportunity to decide whether to accept, mitigate, avoid, transfer, or eliminate the risks arising from an incident. Management could also calculate the residual risk and cost of risk (Năstase & Unchiașu, 2013).

The United States' Office of Comptroller of Currency Banking BC-177 of 1983 required US banks to implement formal disaster recovery plans, which included testing (Herbane, 2010). The US Expedited Funds Availability Act of 1989 required all federally chartered financial institutions to make provisions for next day availability of deposits, including the implementation of business continuity plans (Herbane, 2010).

The World Trade Center attack that occurred in September 2001 in the United States necessitated the need for a reevaluation of business continuity planning (Law & Robson, 2014). That event resulted in the loss of thousands of lives, injuries, and unavailability of buildings and telecommunications. Since then, there have been a plethora of regulations within the financial services sector (Sorial, 2011). Such regulations have come from the Federal Reserve Board, Office of Comptroller of Currency, and the Securities and Exchange Commission. One regulation is the requirement for a business continuity planning and disaster recovery for the financial services sector (Herbane, 2010).

The 2005 Hurricane Katrina caused significant service disruptions in the United States, resulting in over 1,800 deaths and an estimated \$80 million in damage (Baker,

2012). Also in 2005, New Zealand experienced a total telecommunications network failure (Baker, 2012). In a survey of 240 senior executives in the United States about the entity's business continuity planning, it was observed that 21% suspended their business operations on account of the harm caused by a disaster. A well-implemented business continuity plan mitigates service disruptions and negative impact to services (Karim, 2011).

### **Organizations and Business Continuity Planning**

Organizations of all sizes continue to work hard to safeguard their assets should a disaster occur; they recognize that availability of data can give them comfort and help ensure long-term availability of services. However, researchers have noted that while some organizations have business continuity plans to ensure continuity of business, most businesses are far from meeting their objectives when an emergency occurs (Lindström, Samuelson, & Hägerfors, 2010). When organizations were less dependent on information technology, alternative plans for business resumption and activities during an emergency were manual in nature. The plans often included temporarily replacing a crashed computer system with older, paper-based processes, which the workers might already know (Afedzie & McEntire, 2010).

Today, organizations, including the government, are more dependent on information technology. The experiences of the BP oil spill, Hurricane Katrina in the United States, and tsunamis give a clear indication that a disaster can occur at any time without any prior warnings (Ostrander & Lowry, 2012). While organizations are still trying to understand the need for business continuity planning, the internal auditors have been proactive in recognizing the importance of mitigating the impact of disruptive



events (Sarens, Abdolmohammadi, & Lenz, 2012). The internal auditor is in an excellent position to assist with the identification and assessment of risks in the organization (Sarens et al., 2012). The first task might be to get senior management to understand the need for business continuity planning. One approach would be to outline the specific areas within an organization that could be impacted as a result of a disaster: loss of information technology, personnel, business facilities, and third parties with critical business relationships with a government establishment (Baker, 2012).

Crisis may arise from different sources, such as vendors, customers, and organization's facilities. Even information security risks are considered possible business continuity threats. As a result, some organizations are requiring their independent audit organizations implement a business continuity plan to ensure mitigation of disruption of services (Jarvelainen, 2012). Some organizations mitigate service disruptions and ensure continuity of business by controlling their suppliers by requiring business continuity plans, periodic testing of these plans, and relevant certification (Cascardo, 2012). However, for the majority of organizations, certainly, for the large ones, this controlling of suppliers is no longer possible (Cascardo, 2012). With most processing requiring access to increasingly integrated applications and databases, when the system is down, there is no opportunity to do any meaningful work. Researchers have tried to determine how organizations can mitigate the impact of disasters (Afedzie & McEntire, 2010), and some have concluded that there should be a frequent backup of data, preparation of a business continuity plan, periodic meetings, and involvement of all stakeholders (Lehman, 2010).

## Mitigating a Disaster

All stakeholders should participate in the planning for reducing the impact of disasters (Biedrzycki & Koltun, 2012). The stakeholders should include employees, the board of directors, elected officials, customers, consumers, suppliers, and the public (Afedzie & McEntire, 2010). There should also be a risk assessment and impact analysis (Pinta, 2011). Risk assessment would include defining the types of risks or threats to the organization and impact analysis would include analyzing the probability of threats occurring and their impact (Afedzie & McEntire, 2010).

To mitigate hazard, there should be adequate preparedness (McEntire, 2012). One of the first steps is to determine the types of disasters that can occur within the specific vicinity where the government agency resides (McEntire, 2012). This determination could be achieved through consultation with various relevant resources within the organization, such as the internal auditor (de Zwaan et al., 2011). The internal auditors probably understand the functions of their respective agencies more than any other person because of their roles in performing organization-wide risk assessments as a part of determining the auditable areas to be proposed to the board of directors for audit or evaluation (Sarens et al., 2012). This knowledge includes formulating, testing, and exercising disaster plans. There should also be adequate training and discussion with the public and others about disasters and how to mitigate them (Sarens et al., 2012).

McEntire (2012) also discussed the variables that determine the degree of vulnerability. Some groups, individuals, groups, organizations, and communities are more vulnerable than others; however, the vulnerability can be minimized. But to reduce vulnerability, there should be a strategy for reducing risks, susceptibility, and increasing

resistance and resilience (Verchick & Hall, 2011). Other risk-reducing strategies include disaster prevention training and coordination with other coalition partners (Chen & Lee, 2012).

A business continuity plan is a part of long-term planning for an organization (Momani, 2010). An example is the lasting effect created by Hurricane Katrina on August 28, 2005, which caused significant service disruptions (Farber, 2011). Additionally, in a survey of 240 senior executives about the entity's business continuity planning, it was observed that 21% suspended their business operations because of the harm caused by a disaster (Karim, 2011). A well-implemented business continuity plan mitigates service disruption and negative impact to services (Karim, 2011).

Another issue requiring attention is the outsourcing of tax preparation overseas by tax preparers (Desai & Roberts, 2013). The client's concerns have been the security of information and the associated business risks, such as business continuity (Wayman, 2013). Some tax practitioners, especially certified public accountants, have tried to alleviate their clients' concerns by implementing business continuity and disaster recovery plans (Desai & Roberts, 2013). These certified public accountants are regulated by governmental agencies, which must ensure that licensing information is current and available at all times. As a result, there must be continuous assessments of business continuity plans to ensure up-to-date alignment with the long-term goals of the government sector. The internal auditors oftentimes participate in assessing risks but have rarely participated in business continuity planning (Desai & Roberts, 2013).

### **Possible Impact of a Disaster**

A disaster is a significant and unpredictable incident that has the potential to present negative results for an organization. The possible impacts of a disaster to an organization might include legal obligations due to noncompliance with the law, violation of contracts with suppliers, and other interested parties (Bayrak, 2009). Certainly, for the organizations that outsource certain activities, such as data centers, computer help desks, and facility maintenance, there could be enormous financial, legal, and compliance risks related to such associations if a disaster occurs. Therefore, the participation of the internal auditor in the business continuity planning is essential to ensure the identification of internal risks and control gaps associated with the outside service providers (Wayman, 2013).

If an organization, such as a university, goes down because of the impact of a disaster, the concern is what could happen to an employee. Additionally, concerns would be regarding how students, the public, and customers perceive the organization because of the decline as a result of the disaster. For example, in September 2008, Hurricane Ike hit Lamar University, Beaumont, Texas (Beggan, 2011). According to Beggan (2011), the 2000 U.S. Census showed that the city of Beaumont had a population of 113,866 and the university was a significant part of this government's social and economic infrastructure and it was considered a top 10 employer in the city. Owing to the hurricane, the university was closed for about 10 days and suffered approximately \$11 million in damages (Beggan, 2011). Hurricane Ike resulted in the withdrawal of 150 students and tuition, and fee losses of \$480,000 for the 2008 fiscal year (Beggan, 2011). However, this was significantly less because of the lessons learned in the previous

hurricane, Hurricane Rita. Hurricane Rita caused the university to close for 20 days and generated approximately \$38 million of damages (Beggan, 2011).

The 2005 flooding that emanated from Hurricane Katrina in New Orleans created the need for businesses and educational institutions in vulnerable vicinities to reevaluate their plans for disaster recovery (Baker, 2012). Many businesses were incapacitated because of the loss of information spanning several years (Baker, 2012). Similar to the flooding, there have been several power outages in modern industrial societies that had significant economic impact (Omar et al., 2011). Examples were the power outages in the Northeastern United States and Canada in August 2003.

Many insurance companies became insolvent after the 1992 Hawaii and Andrew hurricanes, and the 2004-2005 Florida hurricane season (Carson, McCullough, & Pooser, 2013). The 10 costliest hurricanes in the United States impacted the State of Florida and seven of these events occurred in 2004 and 2005 (Carson et al., 2013). Owing to the impact of the 2004-2005 hurricanes, five insurance companies in Florida became insolvent, and claims totaling \$1 billion were paid by the Florida Insurance Guaranty Association and ultimately passed the costs to the policyholders (Medders, McCullough, & Jäger, 2011). To mitigate the impact of the risks associated with catastrophic events, the United States government has tried to intervene by providing capacity for the funding of these events. However, general participation varies based on the magnitude of loss (Medders et al., 2011).

The Federal Emergency Management Agency (FEMA) provides monetary assistance to organizations when there is a declared disaster (Nicoll & Owens, 2013). FEMA has been active in providing guidance to organizations to ensure adequate

preparation for disasters. There are tips for different disasters, including earthquakes, fire, and flood (Nicoll & Owens, 2013). This agency became part of the U.S. Department of Homeland Security in 2003 in the wake of the 9/11 terrorist attacks. However, policymakers in the United States have held different perspectives on whether the government should be participating in the funding of catastrophic losses (Nicoll & Owens, 2013). For example, the exposure of future earthquakes in the United States is significant, making the management of risk related to disaster an important issue (Medders et al., 2011). Another example is that New York has had a constant threat of tropical storms and in 2005, 15 hurricanes made their way into the North Atlantic region of the United States (Medders et al., 2011). Additionally, the annual cost for disasters arising from power outages to United States consumers is estimated to be \$79 billion (Omar et al., 2011). Therefore, business continuity is one of the most significant concerns of management in the United States, ranking fourth overall (Luftman & Zadeh, 2011). However, studies have indicated that businesses are not ready for possible disasters, and consequently, some do not survive disasters (Luftman & Zadeh, 2011).

Organizations should ensure that critical business processes are available when needed; however, not all processes can be available compared to the costs associated with that function. Additionally, important, but noncritical, processes can be unavailable when needed. As a result, it is important that the right combination of personnel perform a business impact analysis in which all are considered. This exercise helps prepare for possible disruption of services (Akkiraju, Bhattacharjya, & Gupta, 2012).

Mitigating different disruptions stemming from natural or human-made hazards, or technological causes are one of the primary reasons for implementing business

continuity planning (Asgary & Mousavi-Jahromi, 2011). The risk of service disruptions has amplified as organizations continue to depend heavily on technological infrastructure and the majority of businesses have incurred some form of disruptions on account of power outages (Asgary & Mousavi-Jahromi, 2011). In a survey conducted in 2001, it was determined that 70% of the organizations interviewed had had service disruptions emanating from power outages, which generated significant expenses to businesses and their major customers. Furthermore, in a recent survey of international business organizations, it was determined that in excess of 87% had activated their business continuity plans as a result of a power outage. As a result, businesses are taking different measures to ensure adequate protection of information assets. For example, the power outage in the Northeastern United States and Canada on August 2003 resulted in significant economic impacts (Omar et al., 2011). The annual cost resulting from power outages to United States electricity consumers is \$79 billion (Omar et al., 2011).

Organizations and communities are steadily exposed to different types of disasters and as a result, government, healthcare, and academia have been intensifying efforts to ensure mitigation of disasters (Staley et al., 2009). In the late 1970s and 1980s, governments began creating a statutory framework to get involved in mitigating disasters (Hemond & Benoit, 2012). For example, in 1979, the United States created FEMA. In the 1960s, the Canadian government passed its first laws related to mitigating disasters. Also, in 2006, the International Organization for Standardization has also conducted a symposium on how to mitigate disasters (Hemond & Benoit, 2012).

Different types of service disruptions can be very catastrophic to organizations and can negatively affect business organizations. The possible ramifications of the lack

of business continuity plan or an inadequate plan can result in significant risks, which may include the loss of public trust and ultimately the deterioration of critical functions (Guster, Lee, & McCann, 2012). Stakeholders have been scrutinizing organizations' preparedness for a long time (Guster et al., 2012). Another issue faced by organizations is acquiring relevant skills to ensure adequate development, evaluation, and maintenance of the business continuity plan and disaster recovery (Kanellou & Spathis, 2011).

Developing a business continuity plan requires at a minimum risk assessment, a business impact analysis, team development, organization-wide awareness and training, and coordination with government agencies responsible for safety and emergency (Guster et al., 2012). There should be simulations and other exercises. This concept, which is widely used today, was borrowed from the military. Management and employees of organizations have been integrated into plans to mitigate disasters. As a result, they are able to develop management tools and anticipate the impact of disasters and how to manage them (Hemond & Benoit, 2012).

Implementation of key policies would help enhance resilience during a disaster (Kantur & Arzu, 2012). Public and private organizations can embark on new technologies, such as alternative power sources. Additionally, local, state, and federal governments can promote resilience by sharing pertinent information. Such information sharing could strengthen the coordination of mundane services (Kantur & Arzu, 2012).

### **Preparing for a Disaster**

Most organizations are completely dependent on their computer systems and supporting information technology personnel, communication network, files, and program (Grosskopf, 2010). Most organizations also recognize that success could



depend on the capacity to provide information whenever requested by the customers, employers, suppliers, and other stakeholders (Omar et al., 2011). As a result, it has become imperative for the management of these organizations to find effective ways of protecting information assets and plan for swift recovery should a disaster occur (Omar et al., 2011). Disaster planning involves much more than backing up data. Some organizations focus primarily on violence in the workplace, wildfires, and weather, but the landscape of the world has steadily been changing; therefore, organizations need to explore future potential hazards or threats. Even the U.S. government has developed guidance to assist staff in assessing and quantifying the risk hazards such as terrorism, infectious diseases, and evolving risks (Law & Robson, 2014). For example, the U.S. Department of Homeland Security developed the *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks* (FEMA, 2009; Nicoll & Owens, 2013).

An organization should periodically conduct a comprehensive risk analysis that identifies its critical business systems, the risks applicable to those systems, the probability of a disaster occurring, and the effect of the disaster on business functions (Bayrak, 2009). Additionally, there should be a system in place for updating the risk analysis whenever there are major changes affecting these critical systems. Such changes may include information technology, service agreement, and processing requirements. Another component of the risk analysis is identifying critical business processes and the order of restoration if there is a disruption of service. To conduct a good risk analysis, the organization's management must provide the needed support. When such support is lacking or inadequate, resources might not be properly utilized or prioritized. As a result,

the business continuity plan might not align with the overall goal of the organization (Bayrak, 2009).

### **Responding to a Disaster**

The government plays a significant role in the mitigation of disasters. But some government agencies fail to prepare properly and respond to disasters because of inadequate preparation, lack of resources, and other pressing needs (Henstra, 2010). If the government fails to plan appropriately for a disaster, the public's safety, financial security, and self-reliance is significantly affected (FEMA, 2015). Some organizations fail in their response to a disaster on account of a lack of communication and training (Jahangiri, Izadkhah, & Seyed, 2011). In a survey of 200 organizations of all sizes, approximately 57% successfully achieved the recovery time objective, while 33% did not, and 10% could not invoke their business continuity plan (Ojha & Gokhale, 2009). Failure can happen to the government if a business continuity plan is not adequately implemented.

Flooding can play a significant role in our society as a whole. There could be damage to buildings, building equipment, and staff shortages, which could result in the inability to conduct business. For a government agency, such an event could negatively disrupt business. In a recent investigation of senior executives, they rated the government right below their customers as the most important constituency (Johnson, 2010). There have been a number of flood events in the United Kingdom in recent years, and the forecast is that it will increase in the future because of changes related to climate (Wedawatta & Ingirige, 2012). The 2007 flooding affected over 40,000 homes and about

7,000 businesses in the United Kingdom and caused damages of approximately \$4.5 billion (Wedawatta & Ingirige, 2012).

In addition to the United States government's involvement in business continuity planning in the 1970s and 1980s, and the creation of FEMA in 1979, the military started its preparedness in the 1970s in the civil service arena (Hemond & Benoit, 2012). In the 1990s, management was integrated into the concept of preparedness, which resulted in the development of management tools to ensure adequate mitigation of service disruptions (Wedawatta & Ingirige, 2012).

In recent times, the hazards of business interruptions have intensified as businesses have increasingly become dependent on information technology infrastructures that are extensively linked to external resources (Sawalha, Jraisat, & Al-Qudah, 2013). Having an effective business continuity plan ensures mitigation of service disruption and recovery of information assets (Momani, 2010). In essence, while it might not be possible to prevent or eliminate service disruptions, the goal is to reduce the effect of any unforeseen emergencies (Sudmeier, Jaboyedoff, & Jaquet, 2013). For example, during the financial crisis of 1997, especially in Southeast Asia, the Singapore dollar was devaluing quickly against the United States dollar because of adverse currency pressures from other nearby countries, including Thailand (Pheng, Ying, & Kumaraswamy, 2010). In essence, while it might not be possible to prevent or eliminate service disruptions, the goal is to reduce the effect of any unforeseen emergencies (Sudmeier et al., 2013). That negatively affected the economy and reduced business opportunities for construction companies. Additionally, there were bankruptcies, which made it very difficult to obtain financing and maintain positive cash flow (Pheng et al., 2010).

A study conducted by AT&T of 530 entities indicated that 83% of the business leaders who responded indicated their entity had implemented a business continuity plan, 12% reported they did not have a plan and 5% were unsure (Jones, 2011). The preferred solution is to have the right combination of internal controls and tools that will meet the expectations of management in managing the different aspects of the business continuity (Jones, 2011).

### **Summary**

When an organization experiences a disruption of service because of a disaster or other unexpected incident, it is the organization's responsibility to ensure critical functions will continue to operate during or after the incident (Cascardo, 2013). Today, organizations, including the government, are more dependent on information technology. The government sector would rely on business continuity planning to mitigate the impact of such disruption. A large percentage of organizations today fail to understand how business continuity planning could mitigate the impact of service disruptions.

The experiences of the BP oil spill, Hurricane Katrina in the United States, and tsunamis give a clear indication that a disaster can occur at any time without any prior warning (Ostrander & Lowry, 2012). The management of the government agency would be expected to utilize the right resources to ensure proper implementation of the business continuity planning. Implementation of business continuity planning requires an adept knowledge of potential risks and their possible impact on the organization (Glendon, 2013). As a result, there is a need for an independent function whose responsibilities would include informing management and the audit committee about the nature of risks,

the likelihood of the risks, the significant of the risks, and the conditions of the organization's preparedness.

The internal auditor usually understands the activities of the organization and is in a position to provide assurance to management that the business continuity plan is effective, key personnel are knowledgeable of the business continuity plan and of its practical execution, and that it is cost-effective. The internal auditor is in an excellent position to assist in the organization-wide business continuity planning (Sarens et al., 2012).

There are a few studies on business continuity planning. For example, there was a study on the role of the public sector asset manager in responding to climate change. The study discussed the need for public asset managers to mitigate and prepare for future events (Warren, 2010). Another study was an assessment exploration of strategic business continuity planning methods in Michigan small business (Lasecki, 2009). But none of the studies discussed the role of the internal auditor in business continuity planning in the government sector.

### Chapter 3: Research Method

This qualitative single-case study examined the use and the perceived roles of the internal auditor in business continuity planning within the government sector. The problem addressed by this study was the lack of the use and the limited understanding of the perceived roles of the internal auditor in business continuity planning in the government sector. The question that guided data collection and analysis for the present study was:

**RQ1.** What are the perceived use and the roles of the internal auditor in business continuity planning in the government sector?

The government sector is required to address any vulnerabilities that could have a significant impact on operations (Adams, 2008). Exploring the roles of the internal auditor in business continuity planning within the government sector included the examination of planning, implementation, and maintenance of the business continuity plan. As a result, the study necessitated employing the proper research design.

Governments have become more transparent and accountable to citizens. As a result, government services have become more accessible, more efficient, and there is an increased opportunity for citizens to participate in government. The advent of the Internet has provided the government sector the opportunity to find ways of generating more income locally and globally (Baird et al., 2012). Transactions such as taxes, renewal of licenses, or registering to vote can be completed electronically. Additionally, in the last few years, cyber-attacks have steadily increased against both United States government agencies and private organizations (Melnik, 2015). To mitigate the impact of any disaster or disruption of service, a government agency has to implement a business

continuity plan or an emergency plan (Hall et al., 2012). Inadequate preparation by the government could have a significant negative impact on the agency and the public (Haque et al., 2012). The internal auditor helps the government achieve its objectives of serving the public by evaluating and improving the effectiveness of risk management.

To address the research questions posed for this study, a qualitative research method was employed. Schram (2006) identified five qualitative research methods that included narrative, grounded theory, phenomenology, ethnography, and case study. The focus of narrative research is on exploring the life of people or an individual. Narrative research method seeks to develop or build a theory about a specific issue or topic. It is the qualitative equivalent to meta-synthesis, wherein qualitative information and findings are summarized and analyzed to build and strengthen a theory being developed by the study (Finlayson & Dixon, 2008). The method is more relevant when the focus is to explore individual experiences, but not large numbers of anonymous participants. A narrative research is usually used in biography research wherein the focus is on the specific elements of a particular person (Essers, 2012).

The focus of phenomenology is on offering insight into how people or an individual could make sense of a given phenomenon, in a specific context. Phenomenology requires studying and analyzing several individuals who have shared similar experiences. Phenomenology research is focused on 'lived experiences' of participants to provide meaning to the phenomenon being studied. Phenomenology must also be used by the researcher in a manner that portrays a special, open phenomenological attitude (Finlay, 2009). It is only by combining these two criteria that phenomenology can be successfully done. The method is common in the field of

philosophy and education. The individuals must be able to describe their experiences fully. An example is an interaction between an instructor and a parent (Finlay, 2009).

The focus of grounded theory is developing a theory that is derived from and grounded in data from the field. In essence, the goal is to generate a theory. Grounded theory is best used when theory is not available to explain a process or phenomenon (Finlay, 2009). Grounded theory, meanwhile, makes use of the substantive body of grounded research toward a higher, more abstract level. Grounded theory means that the researcher is required to comb through information about the issue or topic at hand to the point of saturation that the results and finding were exhaustive enough for theory building (Barnett-Page & Thomas, 2009).

The focus of ethnography is interpreting cultural behaviors. The method is more relevant when it is used to describe cultural differences (Barnett-Page & Thomas, 2009). In this method, specific components of an observed phenomenon are taken together as a whole to arrive at a sufficient explanation, providing depth and dimension to the issue or topic under study (Barnett-Page & Thomas, 2009). An example would be to describe what people in Canada and the United States do in a given circumstance. The focus of a case study is developing and analyzing one or two cases (Bowyer & Davis, 2012). Under this approach, a topic of interest can be documented and studied in detail, specifically its nature, dynamics, structure, processes, and culture.

Moreover, the case study approach is used to generate an in-depth, multi-faceted understanding of a complex issue in its real-life context and it is also intrinsic, instrumental, and collective (Crowe et al., 2011). A case study is an appropriate approach to research if the case or issue is distinctive enough that it is worth documenting



and reviewing, providing a deep analysis of the issues at hand that, as Crowe et al. (2011) defined, bring out the different facets or dimensions relevant to these issues. Vissak (2010) provided a thorough analysis of the case study approach, specifically applied in international business research. The author discussed how the case study method should be conducted in business research, which, in the present study's case, is about business continuity. An example would be providing a case related to business continuity planning and the perceived roles of the internal auditor. The case has now been fully described and analyzed.

### **Research Methods and Design**

This qualitative research is a single-case study. The utilization of a qualitative methodology facilitated the understanding of the perceived roles of the internal auditor in business continuity planning in the government sector. Qualitative methodology enabled the researcher to collect data that systematically answered the research question, and ultimately produced findings that could be used by the government sector. This case study utilized purposive sampling. Adopting the case study method, the researcher was able to gain insight, and as a result increased the credibility, integrity, and transferability of data collection during the study. Additionally, the case study research methodology appropriate for this study was useful in enhancing reliability and accuracy of the data collected, by limiting inconsistencies resulting from individual interpretations of data collection instruments including file artifacts (Yin, 2009). Moreover, qualitative research has become one of the leading research strategies utilized by disaster researchers (Rodriguez et al., 2007; Stallings, 2007). This methodology is also widely used within the government sector, and several pertinent discoveries have emerged within the emergency

management arena due to the frequent use of qualitative research (Munro, 2011). Jones (2010) used this me

Quantitative methodology pertains to experiments that are aimed at producing internally valid, reliable, replicable, and findings that can be generalized. Therefore, this method involves experiments that tend to mandate control of different variables utilizing observations as a primary data collection tool (Yin, 2009). This study was not experimental, rather interpretive with the primary purpose of an in-depth understanding of the phenomenon researched (Yin, 2009), which involved no mandate to control different variables. To ensure alignment with the research purpose and question, the researcher utilized an interview questionnaire which comprised open-ended questions (Patton, 2002). Additionally, this study included utilizing a small sample of participants from a specific group. Therefore, quantitative methodology was not appropriate for the study. Furthermore, this study did not include clarification of causation and relationship among different variables, which are common in quantitative and mixed-methods research. Therefore, qualitative methodology was best option because the goal of the research study was not to draw a statistical inference based on the findings.

The primary strength of the case study methodology is the focus on a certain phenomenon; but flexible for further exploration. The researcher's focus was on the theoretical framework and not on a large population. A purposive sampling technique was used, and the participants were individuals (Yin, 2009).

A case study is usually data-coded and analyzed with statistics or patterns, which involves understanding the perceived roles of the internal auditor in business continuity planning within the government sector through the collection of raw data and the analysis

of the initial pattern (Glaser & Strauss, 1967). A case study can be past or future-based, depending on the nature of the design (Glaser & Strauss, 1967). However, for the purpose of the current study, the case study design utilized a past perspective to fully understand the perceived roles of the internal auditor in business continuity planning within the governmental sector, which generated new information for the future as a framework for leaders of business continuity planning, as well as for agencies in business continuity planning (Glaser & Strauss, 1967; Yin, 2009).

The target population for this study was internal auditors in the governmental sector from the State of Texas in the United States. According to Glaser and Strauss (1967), purposive sampling is most appropriate for case studies. Purposive convenience sampling is the process of collecting data from a body of people who have experience with the phenomenon under study and are available to the researcher to share their perceptions and experiences (Jones, 2010). This research methodology provided a reasonable assurance that data collected were reliable because of expected limited variability of the interpretation of data collection device (Yin, 2009). Additionally, qualitative research has been regarded as the ideal approach to business continuity and disaster recovery studies (Stallings, 2007). Finally, many of the significant studies and pertinent findings within the business continuity and crisis management field have used qualitative research methodology (Munro, 2011).

Findings arising from the research were valid. To promote this, the researcher avoided being biased by using a questionnaire and one-on-one interviews for all participants (Shank, 2006). There was honesty about personal perspectives, and transparency was exhibited as data were collected and analyzed. The researcher made

sure each participant was not pressured into participating in the research. An informed consent form was signed by each participant prior to the interview (Drost, 2011).

### **Population**

This study examined the roles of the internal auditor in business continuity planning in the government sector. The study participants included government internal auditors in the State of Texas agencies. In order to recruit participants, the researcher obtained the list of internal auditors from the website of the Texas State Auditor's Office. The list included the names, phone numbers, and email addresses of the State of Texas internal auditors working for the State of Texas agencies (Texas State Auditor's Office, 2015). The total number of internal auditors for this study was 253.

The participants of this study were limited to government internal auditors working for the State of Texas agencies and between 18 and 65 years of age. Individuals who were not internal auditors, less than 18 and over 65 years, or not working for the Texas State government were excluded from participating. Participants were selected without consideration of their gender, age, and race. Following this criterion, the sample size was 20.

### **Sample**

The purpose of this study was to understand the perceived roles of the internal auditor in business continuity planning in the government sector. Purposive sampling was used to identify the individuals who were willing participate. This process entailed identifying participants who were to share their perspectives and opinions on the subject under study (Creswell, 2014). The researcher identified each participant by a code name. Twenty internal auditors in the government sector working for the State of Texas

agencies were invited and considered as participants in this study. As emphasized by Creswell (2014), qualitative studies require more focus and a smaller number of participants than quantitative studies do. The researcher initiated contact with potential participants through a phone. During that phone call, the researcher inquired if the individual was between 18-65 years of age. If the potential participant met the age requirement, within 24 hours, the researcher followed up with a recruitment email. Thus, 20 internal auditors were invited with the goal of interviewing 20 internal auditors in State of Texas agencies. All 20 internal auditors were interviewed. This sample was sufficient to provide valuable insights that were used to develop an understanding in the field of research. Semi-structured interviews with the participants provided an opportunity for obtaining deeper information about the roles of the internal auditor in business continuity planning in the government sector (Palliyaguru, Amaratunga, & Haigh, 2010).

### **Materials/Instruments**

The primary instrument for collecting data for this qualitative study was the researcher (Bryman & Bell, 2011). The researcher conducted one-on-one semi-structured interviews using a questionnaire. The utilization of a questionnaire enabled the researcher to collect the data necessary to answer the research question. The aim was to gather the opinions and experiences of the study participants about the roles of the internal auditor in business continuity planning in the government sector (Creswell, 2014). The researcher conducted the interviews with the study participants using open-ended questions (see Appendix F). The researcher developed the questionnaire after considering the research questions and the primary focus of the study (Yin, 2009). The

open-ended questions enabled the participants to answer questions in their words on their perceived roles of the internal auditor in business continuity planning in the government sector.

The first three questions on the questionnaire addressed the significant negative impact of disruptions when a government entity failed to mitigate a catastrophic event due to a lack of proper business continuity planning that considered all risk factors affecting the organization. The second three questions on the questionnaire addressed the obstacles that could prevent an organization from properly involving the right expertise in business continuity planning. The next set of questions in the questionnaire addressed the major roles internal auditors play in an organization, especially in risk assessment. The next set of questions addressed the areas in business continuity planning to be excluded from the internal auditor, if internal auditors were involved in business continuity planning. The last set of questions addressed how the internal auditor's involvement in business continuity planning affect his or her independence and objectivity. The reason was that internal auditor was expected to audit all transactions of an organization, including the business continuity planning.

### **Data Collection, Processing, and Analysis**

After obtaining the approval of Institutional Review Board (IRB), the researcher began initiating contact with the study participants. Using the list of internal auditors from the website of the Texas State Auditor's Office, the researcher identified the names, phone numbers, and email addresses of the State of Texas internal auditors working for the State of Texas agencies (Texas State Auditor's Office, 2015). The researcher purposively selected 20 potential subjects and contacted them via telephone using the

telephone script (see Appendix A). The researcher informed each individual about the purpose of the study, age requirement, estimated duration of the interview, and that participation was voluntary. After verifying the participants' willingness to participate, the researcher followed-up with an email reiterating what was discussed on the telephone (see Appendix B). Each participant elected to do the interview via telephone. The researcher emailed the informed consent form to each participant for signature (see Appendix D). All 20 subjects contacted met the study criteria and agreed to participate. Each interview lasted 30-45 minutes. Each participant was given the option of scanning and emailing or faxing the signed informed consent form. After obtaining the signed informed consent form, an interview date was scheduled. For each interview, the researcher went over the questionnaire questions. All interviews were conducted over the telephone. The research followed the protocol suggested by Yin (2009) regarding data collection procedures, questions, and guide for the report. The protocol stressed the reliability, validity, and credibility of the study Yin (2009). The internal auditor is expected to demonstrate integrity, competence, and due professional care, objective and free from undue influence (Seago, 2015).

Interviews served as the guide for data collection (Hartel & Latemore, 2011). Data collected included interview narrative transcripts and code notes. Analysis of the data help the management, internal auditors, oversight bodies of the government sector under the perceived roles of the internal auditor in business continuity planning. Additionally, the researcher prepared memos to ensure proper documentation of data gathered. Consequently, a coding method for participants ensured confidentiality (Yin, 2009). The data collection lasted approximately 3 months. The researcher created

emergent codes that arose from the analysis of data. The codes were later broken down into sub-codes. Additionally, the researcher jotted down notes of reactions that emerged as a result of the interviews. The researcher used descriptive coding due to limited experience in the use of qualitative data. The second cycle coding used by the researcher was axial method due to the variety of data forms that emanated from the interview. The axial coding process allowed the researcher to disaggregate data into themes and provided an avenue for establishing different linkages and raising new questions for further research (Elo & Kyngas, 2008).

Data analysis consisted reviewing the data collected via the interview questionnaire, utilizing inductive content analysis to sort the information into themes, aligning with the overarching research question, and maintaining internal validity. The researcher did not use deductive content analysis due to a lack of previous research in this area. The first phase of the data analysis was sorting data into themes and patterns for the purposes of coding. The researcher classified, edited, analyzed, and interpreted the themes to ensure credibility of the research. An Excel spreadsheet was used to consolidate and categorize data.

Finally, the researcher developed the findings arising from the study which is in chapter four of this document (Elo & Kyngas, 2008). Additionally, the researcher interpreted data collected and came up with conclusions. Transcripts of the interviews were reviewed by the participants and none provided additional comments or identified issues with the accuracy of the transcript.



### **Assumptions**

A major assumption of the single-case study was that the purposive sampling from a targeted population could be considered a representative sample of government internal auditors in the United States and their perceived roles in business continuity planning. Participants are government internal auditors, and an assumption was that they were not required by management or those charged with governance to participate in this study. After selecting the sample size for the study, an assumption was that at all would participate in this study if they had the time. Furthermore, the assumption was that the participants would be sincere, credible, and open in responding to the interview questionnaire; thereby enhancing the validity of the study (Patton, 2002; Yin, 2009). The researcher, as a CPA and CISA, performed internal auditing outsourcing. As such, there was an assumption during the analysis about the researcher's objectivity in interpreting findings and reducing the investigator's bias (Yin, 2009). Another assumption was selecting a qualitative study for the research problem (Yin, 2009), leading to the factors outlined extensively in the literature review.

### **Limitations**

This case study generated a lot of insight about the perceived roles of the internal auditor in business continuity planning in the government sector. But the inquiry was limited to those internal auditors working in the State of Texas. Therefore, the study was inhibited by the experiences, knowledge, and perceptions of the participants. As a result, the findings of the study might not meet the perceived expectations of past researchers of reliability, credibility, transferability, and validity in the research design, data collection, and data analysis process (Patton, 2002). Additionally, the findings might not apply to all

internal auditors in all government sectors. For example, the lack of the involvement of the internal auditor in business continuity planning could be viewed as an unnecessary step in risk management. Conversely, the involvement of the internal auditor could be viewed as a required process to ensure all risks are adequately considered by the entity. Nevertheless, the primary objective of the case study was not to generalize results across all government agencies in the United States; rather, to fully understand the roles of the internal auditor in business continuity planning in the government sector, specifically in the State of Texas (Yin, 2009). Therefore, the generalization of any findings resulting from this study would be at the prerogative of future researchers (Jones, 2010). Study participants answered interview questionnaire representing an individual's (internal auditor's) perception of the roles of the internal auditor in business continuity planning in the government sector. Twenty participants were purposively sampled from a population of 253. As a result, the purpose sampling methodology used could be subjective; due to the small sample size used in gaining an in-depth understanding of the phenomenon studied and an analysis of large amount of data generated from the research (Yin, 2009).

### **Delimitations**

The study of the roles of the internal auditor in the government sector was a significant assignment. Delimitations were the boundaries of this research study. They were vital in narrowing the scope of the research, which was to understand the perceived roles of the internal auditor in business continuity planning in the government sector. A delimitation was the single-case study research design using purposive sampling; judgmentally selecting a sample of individuals from a population (Yin, 2009), a representative of internal auditors working in the government sector. The choice for data

collection was a questionnaire used in interviewing selected individuals. There was no effort to try to generalize the findings of the study to larger populations. Therefore, the context and geographic area of the study was appropriate in understanding the perceived roles of the internal auditor in business continuity planning in the government sector.

### **Ethical Assurances**

One of the goals of this research was to use measurements that were reliable or consistent. Since there was no simple or one way to measure the reliability of data collected, the researcher asked several different questions to try to achieve the object of the research questions. To promote reliability of information, the researcher asked for clarification whenever determined necessary, just to make sure that the interviewee's response was understood. It was also important to make sure that measurements were valid or accurate. To ensure that interviews were conducted similarly across different participants, the researcher ensured each participant was asked the same set of questions. Thus, semi-structured interviews were used to ensure that the interview process was guided. Information obtained was reported accurately. The researcher only employed triangulation whenever necessary by using a variety of mixes such as interviewing, document analysis, and questionnaires with open-ended questions. The researcher documented the source of data being collected, how it was collected, and how it was used. That ensured a proper audit trail. The researcher ensured the credibility of data by maintaining an extended contact with the respondents. Credibility was improved when data collected from different sources reflected the same findings (Drost, 2011).

Findings should be valid. To promote this, the researcher tried to avoid being grounded in own context and personal perspective (Shank, 2006). There was honesty

about personal perspectives and transparency was exhibited as data were collected and analyzed. To adequately address the research question, a part of validating the work involved embracing the concept of a representative sample (Drost, 2011).

Obviously, it was not practical to interview everyone about the roles of the internal auditor in business continuity planning in the government sector. As a result, the people being targeted were a representative sample of the population affected by the topic under study. The researcher sampled different groups of people. Drost (2011) argued that if the same results were obtained, it would be natural to extend the sample to the population at large. That helped simplify an understanding of the phenomenon under study and further validated the results of the work.

The idea was to demonstrate that the study can be trusted. Things considered included consequences of presence in a setting, selective experience, and engaged subjectivity. Presence in the field was explored including its impact on the credibility of the research. Other considerations included addressing the necessity of attending to some things but not others; and managing and monitoring the subjectivity that influenced the research (Schram, 2006). To ensure the integrity of the research, other possibilities were explored, and those possibilities were supported by the data collected. The researcher fully disclosed the purpose of the study. That was one of the ethics and morality of conducting research. Some researchers believe that the quality of the data gathered may be enhanced by overtly soliciting the cooperation of everyone associated with the subject under study. As a result, they argue that the ultimate acceptance and usefulness of formative information might depend on such prior disclosure and agreement. Related to full disclosure is confidentiality. The report concealed names, locations, and other

identifying information so that people who had been observed or interviewed was protected from harm or punitive action. The researcher sought and obtained an Informed Consent Form or Certificate of Confidentiality (Bryman & Bell, 2011; Rubin & Rubin, 2012).

Prior to interviewing, the researcher for this study outlined a set of issues that were to be explored with each respondent. That was more of informal, conversational interviews. The interview guide (see Appendix E) served as a basic checklist during the interview to make sure that all relevant topics were covered. The researcher was expected to interview up to 20 people. The researcher interviewed 20 people. Each interview varied between 30 minutes to 45 minutes, using a questionnaire (see Appendix F). There were notes as well and memoranda written during the interviews.

### **Summary**

The problem to be addressed by this study was the lack of the use and the limited understanding of the perceived roles of the internal auditor in business continuity planning in the government sector. The government sector is required to address any vulnerabilities that could have a significant impact on operations (Adams, 2008). To address the research questions posed for this study, a qualitative research method was employed. The case study approach is used to generate an in-depth, multi-faceted understanding of a complex issue in its real-life context and it is also intrinsic, instrumental, and collective (Crowe et al., 2011). This qualitative research is a single-case study. This case study utilized purposive sampling. The researcher selected, 20 internal auditors working in the State of Texas agencies to participate in the study. The research followed the protocol suggested by Yin (2009) regarding data collection procedures,

questions, and guide for the report. The protocol stressed the reliability, validity, and credibility of the study Yin (2009). Data analysis consisted reviewing the data collected via the interview questionnaire, utilizing inductive content analysis to sort the information into themes, aligning with the overarching research question, and maintaining internal validity. The assumption was that the participants would be sincere, credible, and open in responding to the interview questionnaire; thereby enhancing the validity of the study. A limitation of the study was that the inquiry was limited to those internal auditors working in the State of Texas. Therefore, the study was inhibited by the experiences, knowledge, and perceptions of the participants. As a result, the findings of the study might not meet the perceived expectations of past researchers of reliability, credibility, transferability, and validity in the research design, data collection, and data analysis process. A delimitation was the single-case study research design using purposive sampling; judgmentally selecting a sample of individuals from a population (Yin, 2009), a representative of internal auditors working in the government sector. The choice for data collection was a questionnaire used in interviewing selected individuals. Data analysis consisted reviewing the data collected via the interview questionnaire, utilizing inductive content analysis to sort the information into themes, aligning with the overarching research question, and maintaining internal validity. The researcher fully disclosed the purpose of the study; one of the ethics and morality of conducting research.

## Chapter 4: Findings

The problem this study explored was the lack of the use and the limited understanding of the perceived roles of the internal auditor in business continuity planning in the government sector. Governments oftentimes worry about continuity as they are under pressure to keep up with the citizen's expectations for optimal services. As a result, a government agency is expected to implement a plan to be followed should an emergency arises (Hall et al., 2012). An adequately implemented plan minimizes the impact of disruption and ensures the quick resumption of operations. Without the involvement of an independent person who understands risk evaluation during the development and implementation of business continuity planning, management of a government agency could assume undesirable business continuity risks. Thus, the primary focus of this was to understand the use and the perceived roles of the internal auditor in business continuity planning within the government sector. The single overarching research question that guided this study was the following:

**RQ.** What are the perceived use and the roles of the internal auditor in business continuity planning?

This chapter outlines the findings arising from an analysis of the data collected with the goal of answering the research question. The subsequent section outlines the findings noted in relation to the theoretical framework. The next section outlines the results of the analysis arising from this study and comparison to previous studies. Finally, an extensive evaluation of the findings arising from this study and its impact on business continuity planning and internal auditing is presented.

## Results

To maintain the anonymity of the study participants, the researcher assigned unique identifiers to each participant. The individual identifier consists of 1-20 numeric numbers. The identifier is used to trace data back to the specific participant. Additionally, the identifier is used to protect the identity of those who participated in the study.

The research required the reviews of the role of the internal auditor in an organization as defined by the Institute of Internal Auditor's International Standards for the Practice of Internal Auditing, the laws establishing the internal audit function and business continuity planning, specifically in the State of Texas, and the business continuity guide published by the Texas State Office of Risk Management. The purpose of the business continuity guide is to ensure that State of Texas agencies can perform its essential functions under all conditions.

Obtaining the business continuity planning guide and the law was very simple owing to the information being publicly available on pertinent websites. The researcher was also able to obtain the names, phone numbers, and email addresses of the State of Texas internal auditors from the website of the Texas State Auditor's Office. A total of 20 participants were interviewed using a questionnaire. Interviews with the participants were not complicated. Overall, the internal auditors contacted were willing to support the study, except for a few who had pressing work issues and could not participate. Additionally, a few other potential participants could not be reached possibly because of other commitments. Eventually, the researcher was able to interview 20 internal auditors in the government sector within the State of Texas. While conducting the interviews, the



participants spoke freely and answered all questions without any resistance. The research identified five themes during the analysis: (a) significant negative impact, (b) obstacles, (c) major roles, (d) areas to be excluded from the internal auditor, and (e) internal auditor's independence (see Table 1).

**Theme 1.** The significant negative impact of a lack of proper business continuity planning for a government sector if a disruption occurs.

**Theme 2.** The obstacles that might get in the way of dealing with disruptions successfully.

**Theme 3.** The major roles the internal auditor plays in an organization, especially the government.

**Theme 4.** The areas within business continuity planning the internal auditor should be excluded, if the internal auditor were to be involved in business continuity planning.

**Theme 5.** The threat to the internal auditor's independence, due to the involvement in business continuity planning.

Table 1

*Themes for Research Question*

Theme	Frequency	Percent
Significant Negative Impact	20	100
Obstacles	18	90
Major Roles	19	95
Areas to Be Excluded From The Internal Auditor	20	100
Internal Auditor's Independence	20	100

*Note: n = 20*

**Demographic characteristics.** All 20 participants are internal auditors in the government sector in the State of Texas and between the ages of 18 and 65.

**Research question.** The question that guided the collection and analysis of data were; “What are the perceived use and the roles of the internal auditor in business continuity planning. There were 5 themes that arose from the analysis.

**Theme 1: Significant negative impact.** All participants (20) emphasized that a disruption of service would have a significant impact on the government sector on account of federal and statutory mandates. They opined that government agencies are expected to provide services to the public, under any condition. Additionally, they all argued that confidential and sensitive data might be lost, and resources such as people and processing environment and associated costs would be negatively affected if there was a disruption. Participants believed there was no alternative for business continuity planning in the government sector and cannot foresee a public sector’s long time success without business continuity planning. Participant 10 summarized:

As with any business including government agencies, if you don’t have a plan, then chances are when something goes bad, it will be much harder to get back to where you are. There should be known consequences on what could potentially happen and a plan in place on what to do if it does occur. It is much better to be ahead of the curve instead of reactionary. If prepared, will cost less, will be back to normal (or as close depending on disruption) sooner, and public perception could be positive versus potentially negative. (Participant 10, personal communication, March 15, 2016)

Participant 6 reasoned that disruption could have a significant impact on critical services, especially “those in healthcare, safety, and state hospitals, and jails.”

Participant 2 affirmed that business continuity planning in the government sector helps to “shorten the duration of the disruption, have a plan of action for various types of disruption” and Participant 7 asserted “We are established by the public to provide services for the public, whether or not there is a disruption.” The planning might include third party agreements, manual workarounds, systemic redundancies, cross-training, back-ups, and transfer of risk with insurance policies. But business continuity planning covers more activities to ensure a government sector succeeds. Participant 8 believed:

An organization needs to prepare for a disruption before it occurs to ensure they are prepared for that disruption. If an organization is providing critical services to the public (public safety, protective services, public assistance, etc.), it is not reasonable to stop providing services until the entire organization is able to recover. Frequently these critical services must be resumed within a matter of hours and not days or weeks. (Participant 8, personal communication, March 1, 2016)

Additionally, Participant 12 supplemented:

In addition, with the rise of cyber-attacks, terrorism, and natural disaster, such as earthquakes, tornadoes, floods, etc, preparing ahead of time has quickly come to the forefront to ensure the agency has an idea of what might happen to overall operations and what steps need to be taken to counteract any type of disruption. (Participant 12, personal communication, March 23, 2016)

Based on the responses from the participants, the researcher identified a sub-theme related to theme (a):

**Sub-theme 1.** This referred to the negative impact of a lack of proper business continuity planning. The negative impact might include the loss of data. Additionally long-term success of the organization could be hampered. There could be health and safety issues. Resources such as revenue, people, facility, and equipment might be affected. The organization might be able to provide critical services, and protective services and public assistance might impacted, if an organization lacked proper business continuity planning (see Table 2).

Table 2

*Significant negative impact*

Negative impact	
Loss of data	Resources affected
Long-term success hampered	Critical services affected
Health and Safety affected	Protective services and public assistance

**Theme 2: Obstacles.** Nineteen of the participants (95%) described the obstacles that get in the way of dealing with disruptions successfully. Some agencies fail properly to conduct a complete analysis of potential disruptions or risks, and as a result, are unable to assess current risk mitigation strategies. As a result, there is little or no consideration of risks that could impede the government sector's ability successfully to minimize the impact of disruptions (Participants 9, 10, 12, 13 & 20). Participant 9 stated, that one of the obstacles is "all the risks not being considered." Additionally, the information used in business impact analysis lacked currency and was not aligned with the agency's mission

and objectives (Participant 13). Additionally, one of the obstacles was the failure to have a plan of action in place (Participants 2, 6, 8, 11, 12, 13, 16, & 20). Participant 2 indicated “lack of planning” as an obstacle. Other obstacles included the lack of adequate resources properly in planning business continuity (Participants 6, 7, 9, 10, 16, 18, & 19). Participant 10 opined obstacles included “high-level staff understanding of what could happen, perception that it won’t happen so don’t need a plan,” and in addition, Participant 19 asserted that obstacles included “the perception that disruption will never happen. Cost, time, and other resources.” Another obstacle mentioned was the lack of testing of the business continuity plan (Participants 1, 9, 13, & 17). Participant 17 believed “Continuity of Operation and Disaster Recovery Plans are seldom fully tested to validate their viability.” Participant 13 summarized that the perceived elements or lack of elements that get in the way of dealing with disruptions successfully include:

Improper planning or not having a continuity plan in place, business continuity procedures not tested at least annually or testing performed is not sufficient, staff not appropriately training on what to do in the event of a disruption, risk assessment fails to identify a potential disruption, critical data, systems, or processes are not defined, and information used in business impact analysis is not current or does not align with the organization’s mission and objectives.

(Participant 13, personal communication, March 15, 2016)

There is also the lack of commitment and the perception that a disruption will never happen (Participants 1, 10, 16, & 19). Some organizations do not follow established communication protocols or are inept at sharing information (Participants 2,

10, & 12). Participant 10 reasoned one of the obstacles was “the lack of communication with everyone on how, what, when, who is responsible, etc. on if disruption occurs.”

Another major issue was assigning inept personnel to deal with disruptions (Participants 2, 4, 5, & 9). Participant 2 stated that one of the obstacles was ‘the right personnel not being involved in the process.’ Many organizations do not adequately train staff on what to do in the event of a disruption; critical data, systems, or processes are not defined (Participants 2, 12, & 13). Some participants reported that some key stakeholders and process owners do not have business continuity planning as a priority compared to other business objectives within the government agency (Participants 6, 9, 11, 17, 18).

Two participants believed management would not want the internal auditor to be involved with business continuity planning owing to threats to independence (Participant 3 & 12). Participant 12 stated, “Management may be concerned that Internal Audit is just to give them findings or they may be concerned that Internal Audit’s participation could impair their independence affecting the ability to audit the BCP [business continuation plan] and processes in the future.” Seven participants (35%) believed management would be leery about getting the internal auditors’ perspective in the development and implementation of business continuity planning because they would not provide value because of knowledge gaps and that the internal auditors would get in their way of their planning. Another participant reasoned that the internal auditor might not have a strong working relationship with individuals in different business units just because they are auditors and are always scavenging for mistakes that could result in future audits. Participant 2 stated, “Management could want to keep the internal auditor out of the planning process if there are gaps that management knows exist.” Therefore,

management might not be receptive to the internal auditor's participation since that might create more issues. One participant opined that management's lack of awareness of the internal auditor's role in the organization could result in not involving them in business continuity planning (Participant 12). Participant 12 specifically indicated "top decision makers are not identified with both roles and appropriate authority defined."

**Sub-theme 2.** This referred to the obstacles that get in the way of dealing with disruptions successfully. There might be failure to conduct analysis of risk affecting the organization. An organization might have a plan but never practiced it. There could be sentiment that a disaster would not happen, the internal auditor would be provide value, there might be knowledge gap between management and staff of an organization and the internal auditor in terms prioritizing risks affecting the organization. An organization's risk assessment might be current or not even have a plan in place. There could be a lack of resources to implement a plan. There might be lack of training, and inept people entrusted with plan, lack of communication , poor relationship with staff, and threat to the independence of the internal auditor (see Table 3).

Table 3

*The obstacles that get in the way of dealing with disruptions successfully*

Obstacles	
Failure to conduct risk analysis	Failure to have a plan in place
Plan exists but not practiced	Lack of resources to properly plan
Disaster is not going to happen	Lack of training
Not high on priority list	Threat to independence and other issues
Internal Auditor is not providing value	Inept people entrusted to plan
Knowledge of gap	Lack of communication
Lack of currency or alignment	Poor relationship with staff

**Theme 3: Major roles.** Nineteen of the participants (95%) believed the internal auditor should play a major role in business continuity planning in the government sector. They reasoned that the internal auditor has a broader and more independent view of the organization and could provide valuable insight on areas that are at risk. Ten of the participants (50%) indicated that the internal auditor should be involved because of their experience in risk identification and objectivity in assessing risks (Participants 2, 5, 7, 8, 10, 12, 13, 14, 17, & 18). Participant 2 believed

The internal auditor has a broad view of operations and could provide gap analysis to ensure all facets are covered. The internal auditor could also provide insight on areas that have been audited in the past that are at risk for business continuity planning.

Participant 18 stated, "Internal Audit are control experts and could help identify key business continuity risk and control gaps." Participant 12 added:

Internal Audit can assist by reviewing the risk assessment/analysis for overall adequacy and appropriateness, can assist with BIA, and can audit/evaluate the plan to identify weaknesses and ensure it is up to date and relevant. Overall, Internal Audit plays a critical role in offering objective feedback by assessing whether the program provides effective coverage to protect the agency from harm before/when a significant disaster occurs. (Participant 12, personal communication, March 23, 2016)

Six participants (30%) emphasized that internal auditors understand the entire organization on account of their roles due to their roles. As a result, they understand risks that might be neglected by management and are in a position to provide some pointers to



management (Participants 1, 2, 5, 7, 10, &14). Participant 7 indicated “Internal Auditor understands risks that may be overlooked by management. Understands the entire organization and can provide some pointers to management.”

Several participants also reasoned that the internal auditor position ensures that the business continuity planning process is adequately planned, in place, and provides for periodic testing (participants 3, 4, 6, 7, 9, 10, 11, 12, 14, 15, 16, 19 & 20). Participant asserted “Internal Auditor can provide an unbiased, objective opinion on the risk.” One participant indicated that the internal auditor should assist management by reviewing the risk assessment, overall adequacy, and appropriateness of the business continuity plan. Because of their enterprise-wide risk perspective, the internal auditors can help inform those charged with governance regarding the government entity’s data, systems, and processes that are critical and should be protected (Participant 17). One participant argued that the internal auditor does not necessarily have to participate in the development of business continuity planning, but reasoned that in the absence of strong continuity structure, it is the responsibility of the business area to determine risk, but if the entity does not address the risk then the internal auditor has to identify risk (Participant 8).

**Sub-theme 3.** This referred to the reason for the internal audit to play major roles in business continuity planning. The internal auditor understands the organization well, risks, and risk assessment, provides assurance to management and board, has a broader of the organization, and is expected to be objective and independent in his or her view of the organization (see Table 4).

Table 4

*The reason for the internal auditor to play major roles in business continuity planning*

Major roles	
Understands the organization well	Understanding of risks
Objective independent view	Assurance to management and board
Understands risk assessment	Broad view of organization

**Theme 4: Areas to be excluded from the internal auditor.** All participants believed the internal auditor should not be involved in making management decisions related to business continuity planning. They should only participate in an advisory capacity. All participants reasoned that the internal auditor could provide an unbiased opinion during business continuity planning since they are considered control experts. There were reminders that internal auditors have the expertise in risk assessment and mitigation owing to their overall knowledge of the organization. As a result, they are in a position to validate the information provided by various sections of the government sector by identifying key business risks and control gaps performing an audit process when necessary, in addition to assisting executive management in identifying priorities that impact the organization (Participants 2, 5, 7, 8, 10, 12, 13, 14, 17, & 18). Participant 13 stated:

Internal Auditors should be consulted to assist in identifying risk and control information to perform business impact analysis. In addition, Internal Audit staff may conduct assurance or advisory engagements before, during, and after an interruption to assess the effectiveness of business continuity planning.

(Participant 13, personal communication, March 15, 2016)

A participant identified the steps to be considered in the development and implementation of business continuity planning which might consist of defining critical functions, identifying risks and strategies for mitigating those risks, prioritization of critical services, the identification of resources necessary to deploy those services, evaluating different recovery strategies, implementing, testing and maintaining the plan. The participant indicated that these could be completed without the assistance of the internal auditor of the organization, but “probably not the wisest thing to do. The internal auditor’s input is essential to ensure all risks are considered” (Participant 19, personal communication, March 17, 2016). Participant 2, 5, 7, and 18 indicated that update and maintenance of the business continuity plan should be completed by management or staff other than the internal auditor because they are considered management functions. Participant 5 opined “If the internal auditor should be excluded from any activity, I would suggest update and maintenance as that is truly an operational activity” and Participant 18 added that internal auditor should be excluded from “update and maintenance of the plan as internal audit would then become part of control.” Participants 2, 11 and 16 believed disaster recovery and strategy should be completed by management and staff other than the internal auditor since they are considered management functions (Participants 2, 11, & 16). Participant 2 stated,

The internal auditor should be involved in the analysis and testing phases as they are areas that can provide better objective insight to management. Disaster recovery plan and update and maintenance are more of a management function and not an assessment function.

Two participants also believed that the business impact analysis should be completed by management or staff other than the internal auditors because it is considered a management function. But the internal auditor should provide critical consulting roles in these areas to ensure objectivity so that the planning process is more efficient and effective owing to the wealth of knowledge in performing risk assessment and identifying risks, and help validate, mitigate, diffuse intra-agency competing interests, and provide objective information to executive management and those charged with governance (Participants 4 &17). Participant 17 summarized:

We must ensure our independence by not developing the plans or getting involved in management decisions. Our role should be one of review and assessment, providing management with information by which they can make informed decisions. The biggest risk to an organization for not involving the internal auditor in business continuity planning is that professional and independent resources are not taken advantage of. The unbiased, third-party perspective can help management make informed decisions, and perhaps diffuse internal, cross-organizational conflict. (Participant 17, personal communication, March 8, 2016)

***Sub-theme 4.*** This referred to the areas in business continuity planning the internal auditor should be excluded if they were to be involved in business continuity planning. The internal auditor should be excluded from making management decisions, participating in business impact analysis, updating and maintenance of the plan, and disaster recovery and strategy. These areas should be the responsibility of management (see Table 5).

Table 5

*The areas the internal auditor should be excluded*

Areas to be excluded	
Making management decisions	Update and maintenance
Business impact analysis	Disaster recovery and strategy

**Theme 5: Internal auditor's independence.** All participants agreed that the independence of the internal auditor would not be impaired due to participation in business continuity planning. They argued, however, that there could be a threat to independence depending on the role of the internal auditor. They all believe the best safeguard would be to have an understanding up front with the management of the government sector outlining the roles of the internal auditor as a consultant, not as someone making decisions for management, in the process. Participant 2 stated:

One of the necessary safeguards to mitigate the impairment of independence is to ensure that there is a consulting agreement or Memorandum of Understanding to identify roles that the internal auditor will play in the process. Ensure that the internal auditor is providing only assurance services and not participating in management functions. (Participant 2, personal communication, March 17, 2016)

Additionally, Participant 18 emphasized the importance of instituting necessary safeguards to ensure mitigation of impairment of independence:

There should be clear statement of work that is documented and communicated to executive management. Internal Auditor cannot be responsible for the business continuity plan including being part of the process or determining which business

operations should take priority. (Participant 18, personal communication, March 26, 2016)

One participant stated that “the auditor should never direct the group in a specific direction (make a decision), but instead provide information that the group can use to make their own decisions” (Participant 6). The participant added that roles should be “here is the process you should consider performing” in lieu of “here is the process you should use and here is the format you should use” (Participant 6).

Thirteen participants (65%) believed the reactions of those charged with governance could be negative or positive, depending on their understanding of the roles of the internal auditor in business continuity planning within the government sector. But they suggested that it is the duty of the internal auditor to explain to management and those charged with governance why the internal auditor should play a role in business continuity planning (Participants 1, 2, 3, 4, 5, 7, 8, 10, 11, 12, 14, 15,16, & 19). Participant 5 stated, “Those charged with governance might be surprised because they have preconceptions about the role of internal audit.” Participant 15 stated “It is up to Internal Audit to explain to senior management why internal audit should have a role. They can then agree to what those roles will be if it is an advisory versus an assurance service.” Participant 16 stated, “It is the duty of the Internal Auditor to point management and those charged with governance to the Internal Audit Charter which spells out the responsibilities of the Internal Auditor.” Six participants (30%) believed those charged with governance should welcome the knowledge of the internal auditor and the assurance that the plan is appropriate (Participants 1, 9, 12, 16, 17 & 18). On the other hand, Participant 18 stated: “Those charged with governance would have positive

reactions due to the greater level of assurance that the plan is appropriate and sufficient through an independent assessment.” Participant 12 stated, “They may feel a sense of assurance that the plan was developed based on relevant risks and analysis, (if audited) that the plan is complete and adequate, and that they are informed on the progress, etc.”

**Sub-theme 5.** This referred to the independence of the internal auditors in an organization. The board welcomes the independence of the internal auditor. Also, the business continuity plan is usually developed based on risk identification and analysis. However, there could be a threat to the independence of the internal auditor for participating in business continuity planning. As a result, the internal auditor’s participation might or might not resonate well with the board. The internal auditor would mitigate the impairment of independence by using a Memorandum of Understanding (M.O.U) signed between management and the internal auditor prior to participating in business continuity planning (see Table 6).

Table 6

*Independence of the internal auditor*

Independence	
Independence not impaired if M.O.U	Threat to independence
Positive reactions by the board	Board welcomes independence
Positive and Negative reaction by board	Plan developed based on risk

**Evaluation of Findings**

In this section, the findings arising from this study are evaluated. First, the findings were appraised in light of current theory. This study and findings were compared to past research. Finally, how business continuity planning is affected by this

research is presented. Analysis of the data resulted in the manifestation of five themes. The themes were (a) significant negative impact, (b) obstacles, (c) major roles, (d) areas to be excluded from the internal auditor, and (e) internal auditor's independence. The following is an evaluation of theme findings in comparison and contrast with current research studies.

**RQ.** What are the perceived use and the roles of the internal auditor in business continuity planning in the government sector?

**Theme 1: Significant negative impact.** When a government sector falls short of implementing the required and appropriate measures to mitigate disruptions, the potential risks can be great (Hall et al., 2012). This failure might result in an ill-advised response to an emergency and the possible use of limited resources improperly (DHS, 2006; Ojha et al., 2013). Evidence from this theme indicates that organizations are concerned about people, property damage, and monetary loss, but not enough attention is given to confidential and sensitive information that can potentially lead to negative exposure (Ojha et al., 2013; Verchick & Hall, 2011).

**Sub-theme 1.** When asked to about the negative impact of a lack of proper business continuity planning, some participants indicated that there might be the loss of data. Additionally, long-term success of the organization could be hampered. There could be health and safety issues. Resources such as revenue, people, facility, and equipment might be affected. The organization might be able to provide critical services, and protective services and public assistance might be impacted, if an organization lacked proper business continuity planning.



**Theme 2: Obstacles.** Some organizations fail properly to conduct a complete analysis of potential disruptions or risks, and as a result, they are unable to assess current risk mitigation strategies event (Raman et al., 2011). The current study found that some government agencies do not consider risks that could impede the government sector's ability to mitigate the impact of disruption successfully. Additionally, one of the obstacles was the failure to have a plan of action in place and lack of resources to properly plan business continuity and that business continuity plans are seldom tested (Chandra et al., 2013).

**Sub-theme 2.** When asked about the obstacles that get in the way of dealing with disruptions successfully, findings from the current study also indicated that there is a lack of commitment, perceptions that disruption will not happen, improper communication, and inept personnel being assigned to deal with disruptions. Participant 9 stated, "The right personnel are being involved in business continuity planning." The findings additionally indicated that some key stakeholders and process owners did not have business continuity planning as a main concern compared to other business objectives within the government agency. Participant 6 opined, "I think some organizations including government agencies lack planning properly for disruptions and do not regard business continuity planning as important as other issues." Additionally, the information used in business impact analysis lacked currency and was not aligned with the agency's mission and objectives. The findings further indicated that management of an organization including the government sector would not want the internal auditor to be involved with business continuity planning owing to threats to independence. Finally, the findings indicated that management would be leery about getting the internal auditors'

perspective in the development and implementation of business continuity planning because they would not provide value because of knowledge gaps and internal auditors getting in the way of their planning.

Four participants believed management would not want to involve the internal auditor in business continuity planning because of threats to the internal auditor's independence. Another participant reasoned that the internal auditor might not have a strong working relationship with individuals in different business units just because they are auditors and are always scavenging for mistakes that could result in future audits. Therefore, management might not be receptive to the internal auditor's participation as that would create more issues. One participant opined that management's lack of awareness of the internal auditor's role in the organization could result in not involving them in business continuity planning (Kanellou & Spathis, 2011; Soh & Martinov-Bennie, 2011).

**Theme 3: Major roles.** Findings indicated that the internal auditor should play a major role in business continuity planning in the government sector. They reasoned that the internal auditor has a broader view of the organization and could provide valuable independent insight to management and those charged with governance in areas that are at risk (Schneider et al., 2012; Stefaniak et al., 2012; García et al., 2012). The internal auditor who performs auditing of all the activities of an organization should be in a better position to understand the functions of the governmental entity and can provide independent information regarding risks and the effectiveness of the business continuity plans and whether or not the cost is effective (Chambers, 2014; Dickey et al., 2006; Zain,

Zaman, & Mohamed, 2015). As such, the internal auditor is considered a significant part of an organization's internal control structure (Wines, 2012; Zerni, 2012).

**Sub-theme 3.** When asked about the reason for the internal audit to play major roles in business continuity planning. The participants overwhelming indicated that the internal auditor understands the organization well, risks, and risk assessment, provides assurance to management and board, has a broader of the organization, and is expected to be objective and independent in his or her view of the organization.

**Theme 4: Areas to be excluded from the internal auditor.** Current research indicated that there are specific areas in business continuity planning within the government sector from which the internal auditor should be excluded. They included identifying risks and strategies for mitigating those risks, prioritization of critical services, the identification of resources necessary to deploy those services, evaluating different recovery strategies, implementing, testing and maintaining the plan. In these cases, the internal auditor should be used as an advisor because of their overall understanding of the risks facing the organization. In essence, one of the internal auditor's primary role is assessing and evaluating risk within the organization (Dickins & Daughterty, 2012; Novriansa, & Riyanto, 2016). Participant 8 stated, "Internal auditors should provide options that they are aware of, but should not recommend a specific option."

**Sub-theme 4.** When asked about the areas in business continuity planning the internal auditor should be excluded if they were to be involved in business continuity planning. The participant expressed their sentiments that the internal auditor should be excluded from making management decisions, participating in business impact analysis,

updating and maintenance of the plan, and disaster recovery and strategy. These areas should be the responsibility of management.

**Theme 5: Internal auditor's independence.** Findings from the current study indicated that the independence of the internal auditor would not be impaired on account of participation in business continuity planning. There could be a threat to the independence of the internal auditor, however, depending on the role the auditor played in business continuity planning. As a safeguard against the impairment of the internal auditor's independence, there should be an understanding up front with the management of the government sector outlining roles of the internal auditor as a consultant, not as someone making decisions for management. In essence, the internal auditor's role is to assess and evaluate risks, not making decisions for management which ultimately could impair the independence of the internal auditor (Abbott, Daugherty, Parker, & Peters, 2016; D'Onza, Selim, Melville, & Allegrini, 2015; Zaharia et al., 2014).

**Sub-theme 5.** When asked how the internal auditor's independence would be affected if allowed to participate in business continuity planning, the participants opined that the independence of the internal auditors is vital in an organization, even though the business continuity were based on risk identification and analysis . Although the board welcomes the independence of the internal auditor, there could be a threat to the independence of the internal auditor for participating in business continuity planning. As a result, the internal auditor's participation might or might not resonate well with the board. The participants expressed confidence that the internal auditor would mitigate the impairment of independence by using a Memorandum of Understanding (M.O.U) signed

between management and the internal auditor prior to participating in business continuity planning.

**Comparison to past research.** Past literature supported the importance of business continuity planning to ensure that the government sector is ready to respond to a service disruption or emergency. Additionally, the negative effects of a service disruption or disaster can be significant to the government sector, which might include casualties or even death, negative public perception, property damage, and monetary loss (Day, Melnyk, Larson, Davis, & Whybark, 2012; Haddow et al., 2011). Therefore, when proper skills and knowledge are not used to ensure continuity of business, there is the risk of unsuccessful response to a disaster, and potentially significant losses (Haque et al., 2012; Kusumasari et al., 2010).

Findings from the current study also indicated that the government sector does not consider risks that could impede the government sector's ability to mitigate the impact of disruptions successfully. This assertion contrasts with past research which showed that the government considers different types of risks. Additionally, sometimes staff are not adequately trained on what to do in the event of an emergency (Chen, & Lee, 2012).

Past research focused on the risks facing organizations today. For example, there were risks related to natural disasters such as wind, hail tornadoes, and lightning (Goudsmit, 2012). There were past findings on the need for public asset managers to mitigate and prepare for future, business continuity planning management in local governments, an exploration on business continuity planning in Michigan small businesses, how to ensure continuity of business in general small and medium businesses,

and on education technology (Botha & von Solms, 2004; Lasecki, 2009; Mekdeci, 2011; Smit, 2005; Warren, 2010).

Past research also supported the findings in the current study which included developing and implementing a business continuity plan to mitigate potential loss through the identification, prioritization, and safeguarding of critical assets of the business, not only information technology (Hoong & Marthandan, 2014). Additionally, there were studies supporting the findings in the current study that internal auditors understand and have a broader view of potential risks affecting the organization and the potential impact of any loss (Schneider et al., 2012; Stefaniak et al., 2012). Business continuity is still an emerging concept (Pelfrey & Kelley, 2013). There was no sufficient past literature on the perceived roles of the internal auditor in business continuity planning within the government sector.

Prior studies recognized the expertise of the internal audit identifying and prioritizing risk, but there was no sufficient work on the perceived roles of the internal auditor in business continuity planning within the government sector (Schneider et al., 2012; Stefaniak et al., 2012).

### **Summary**

The purpose of this qualitative single-case study was to understand the use and the perceived roles of the internal auditor in business continuity planning within the government sector. The results of the study arose from data analysis of 20 interview questionnaires derived from a theoretical sample. The steps included a pattern of response matching, coding, and labeling of themes arising from the analysis. The data analysis resulted in five themes. The five themes for the overarching research question

included: (a) significant negative impact, (b) obstacles, (c) major roles, (d) areas to be excluded from the internal auditor, and (e) internal auditor's independence.

The findings arising from the study indicated that potential risks could be great when a government sector falls short of implementing the required and appropriate measures to mitigate disruptions, that might result in improper response to an emergency and possible use of limited resources undesirably. Organizations are concerned about people, property damage, and monetary loss, but not enough attention is given to confidential and sensitive information that can potentially lead to negative exposure.

Findings from past literature indicated some similarities with the current study in terms of the need for government sector implementing certain measures to ensure mitigation of disasters and other disruptions. Some organizations fail properly to conduct a complete analysis of potential disruptions or risks, and as a result, they are unable to assess current risk mitigation strategies. Findings from the current study also indicated that the government sector does not consider risks that could impede the government sector's ability to mitigate successfully the impact of disruptions owing to other competing priorities and the lack of adequate resources needed to plan business continuity properly. Additionally, business continuity plans are seldom tested. There is also the perception that disruption will never happen, a lack of commitment or proper communication, and unqualified personnel being assigned to deal with disruptions

Additionally, the information used in business impact analysis lacked currency and was not aligned with the agency's mission and objectives. The findings also indicated that some management of organizations, including the government sector would not want the internal auditor to be involved with business continuity planning

because of threats to the internal auditor's independence. Findings from the current study also indicated that management would be leery about getting the internal auditors' perspective in the development and implementation of business continuity planning because they would not provide value because of the knowledge gaps and that the internal auditors would get in their way of their planning. Additionally, the internal auditor might not have a strong working relationship with individuals in different business units just because they are auditors and are always scavenging for mistakes that could result in future audits. As a result, management might not be receptive to the internal auditor's participation since that might create more issues. Another issue was the perception that management's lack of awareness of the internal auditor's role in the organization could result in not involving them in business continuity planning.

The findings indicated that the internal auditors should play a major role in business continuity planning in the government sector because they have a broader view of the organization and might provide valuable insight on areas that are at risk. Although there could be a threat to the internal auditor's independence for participating in the business continuity planning; as a safeguard and to dilute such perception, there should be an understanding up front with management of the government sector clarifying that the roles of the internal auditor would be as a consultant and not as someone making decisions for management. The internal auditor's participation would ensure management and those charged with governance are getting objective information related to business continuity planning. Such participation could be viewed positively or negative by those charged with governance, depending on their understanding of the roles of the internal auditor.



The specific areas internal auditors could be involved in business continuity planning included identifying risks and strategies for mitigating those risks, prioritization of critical services, the identification of resources necessary to deploy those services, evaluating different recovery strategies, implementing, testing and maintaining the plan. In these cases, the internal auditor should be used as an advisor on account of their overall understanding of the risks facing the organization. Past studies supported the findings of the current study that internal auditors better understand and have a broader view of the risks affecting the organization and the potential impact. But there was no sufficient past literature on the perceived roles of the internal auditor in business continuity planning within the government sector.

## Chapter 5: Implications, Recommendations, and Conclusions

The purpose of this qualitative single-case case study was to understand the use and the perceived roles of the internal auditor in business continuity planning within the government sector (Hall et al., 2012). But without the involvement of those with the expertise related to risk assessment and evaluation, management of a government agency could assume undesirable business continuity risks. An internal auditor is an independent person who has a broader view of the organization and understands risk evaluation. This position reports directly to those charged with governance and also ensures a decision has been adequately documented (García et al., 2012). The internal auditor's qualifications are essential in determining the ability to perform his or her duties adequately, which includes at least a four-year degree, certifications as Certified Internal Auditor, Certified Public Accountant, or Certified Information Systems Auditor. Internal auditors are required to participate in continuing professional education (Abbass & Aleqab, 2013; Kamel & Elkhatib, 2013). There is no sufficient literature on the perceived roles of the internal auditor in business continuity planning in the government sector.

Governments oftentimes are ill-prepared to handle disasters because of a lack of adequate resources, other competing issues, and improper preparation for catastrophic events (Donahue, Cunnion, Balaban, & Sochats, 2012; Jensen, 2011; Renaud, 2012). Therefore, they apply their resources on more critical issues. Even the *Nationwide Plan Review* conducted by the Department of Homeland Security determined that only 10% of business continuity plans are adequate to mitigate the effect of disasters (DHS, 2006). The shortcomings identified included a lack of proper documentation of risks and the probability of occurrence and consideration of critical segments of the public (DHS,

2006). The lack of adequate preparation could pose a significant challenge to the government should an event occur (Ericksson, 2009). Furthermore, these shortcomings could overtax the needed resources that are earmarked for mitigating the effect of catastrophic events and possibly the loss of revenue. Additionally, catastrophic events could result in unnecessary distress, harm, and the public perception of the government could plummet abysmally (Kusumasari et al., 2010; Shughart, 2011). These shortcomings are usually because of the lack of planning properly. Proper planning includes proper identification of risks, the probability of occurrence, impact analysis, consideration of response alternatives, and testing and maintenance (Kruger, 2009; Kusumasari et al., 2010). Consequently, the problem addressed by this study was the lack of the use and the limited understanding of the perceived roles of the internal auditor in business continuity planning in the government sector.

Governments are usually concerned about continuity since they are under pressure to keep up with the citizen's expectations for optimal services. Additionally, globalization and technological advancements have changed how governments do business (Nasim & Sushil, 2010). For example, Malaysia had never experienced a tsunami until its occurrence in 2006 and because of the lack of proper planning, experience, and expertise, the government was not prepared to mitigate the disruption arising from that event (Raman et al., 2011). Potential risks to the government might include the loss of mission critical data, displacement of workers, and unavailability of facilities due to catastrophic events (Gourio, 2012).

The purpose of this qualitative single-case study was to understand the use and the perceived roles of the internal auditor in business continuity planning within the

government sector. The study identified the obstacles that could negatively affect the resumption of service when there is a disruption. The focus of this case study was examining the roles of internal auditors in the governmental sector, specifically, for the State of Texas in the United States. The study was a single case qualitative research with an embedded unit of analysis that comprised 20 internal auditors in the government sector, specifically, the State of Texas. The study utilized an interpretive approach and theoretical sampling (Patton, 2002; Suri, 2011; Yin, 2009). Data sources utilized for this case study were document reviews and interviews. Five themes surfaced from data analysis: (a) significant negative impact, (b) obstacles, (c) major roles, (d) area to be excluded from the internal auditor, and (e) internal auditor's independence.

But the inquiry was limited to those internal auditors working in the State of Texas. Therefore, the study was inhibited by the experiences, knowledge, and perceptions of the participants. As a result, the findings of the study might not meet the perceived expectations of past researchers of reliability, credibility, transferability, and validity in the research design, data collection, and data analysis process (Patton, 2002). Additionally, the findings might not apply to all internal auditors in all government sectors.

A limitation of this study was that the inquiry was made only to internal auditors working in the State of Texas. Therefore, the study was inhibited by the experience, knowledge, and perceptions of the study participants. As a result, the findings of the study might not meet the perceived expectations of past researchers of reliability, credibility, transferability, and validity in the research design, data collection, and data analysis. Additionally, the findings might not apply to all internal auditors in all

government agencies. but that was not the objective of this study. Rather, the goal was fully to understand the roles of the internal auditor in the government sector, specifically the State of Texas. Nevertheless, the research design could apply to other government agencies in the United States with the reasonable expectation of achieving similar results. For example, involving the internal auditor in business continuity planning could be viewed as a needless step in business risks evaluation by management. On the other hand, soliciting the expertise of the internal auditor could be viewed as a necessary process to mitigate adequately the risks considered by management. However, the generalization of research findings would be at the discretion of future researchers (Jones, 2010).

There were measures in place during the research to ensure ethical assurances throughout the research. The researcher began collecting data after obtaining the approval of the IRB for the current study. Each participant signed an Informed Consent form indicating agreement to participate in the study. A questionnaire was utilized for the interview. All participants were briefed about the purpose of the study and data collection (APA, 2010, Hicks, 2011). Additionally, all participants were informed of their rights not to participate or to terminate at any time without any negative ramifications (Paul, 2012).

The participants' privacy and confidentiality were deemed very important; as a result, fictitious names of people and government agencies were used. No identifiable information was utilized throughout the study (Hicks, 2011). The researcher was the only one that had access to the list linking participants and their specific government agencies. Data obtained during this study were kept in a password-protected computer

and in a locked cabinet, and only the researcher has access to it. All data will be deleted and destroyed seven years after the completion of the study. Additionally, the researcher has made sure the dissertation manuscript includes no identifying information; (Matuk & Young, 2011). Therefore, there is minimal risk of harm resulting from this research (Arwood & Panicker, 2011).

The documentation and reporting of research results included the necessary information. Additionally, data were not exploited, and there was no evidence of bias in analysis and reporting of findings (APA, 2010). The researcher was able to achieve this by carefully reviewing the information obtained during the research study which included tracing back to the appropriate source documents and cross-referencing to report. This procedure provided reasonable assurance that errors would be prevented or detected and that findings were presented accurately (APA, 2010; Hicks, 2011).

This chapter includes a discussion of implications, recommendations, and conclusion of the research study. Implications include discussions on the results of the study in relation to the purpose and problem that warranted the study. Additionally, recommendations are structured around theoretical contribution and practical application, best practices, and proposals for future research. Finally, the conclusions arising from this study are presented.

### **Implications**

The implications arising from the results of this study were addressed below. The overarching research question is stated again, followed by (a) any potential limitations that affected the interpretation of the results; (b) the significance of the findings and the

response to the study problem and purpose using the five themes identified in the analysis; and (c) how the study contributes to the existing literature.

**Research question.** What are the perceived types and possible impacts of service disruptions within the government sector, obstacles that could negatively affect the resumption of service when a disaster occurs and the roles of the internal auditor in business continuity planning? The themes that arose from this study addressed the overarching research question. The results from this study depicted several key points related to the research question.

**Potential limitations.** As stated in Chapter 3, a limitation of this that the inquiry was made only to internal auditors working in the State of Texas. Therefore, the study was inhibited by the experience, knowledge, and perceptions of the study participants. As a result, the findings of the study might not meet the perceived expectations of past researchers of reliability, credibility, transferability, and validity in the research design, data collection, and data analysis. Additionally, the findings might not apply to all internal auditors in all government agencies. But the primary objective of the study was to understand the roles of the internal auditor in the government, specifically, for the State of Texas. Though the results of the study could be applied to other government agencies in the United States or other parts of parts of the world with the reasonable expectation of achieving similar results; this was not the objective of the study.

*The significance of the findings and the response to the study problem and purpose using the five themes identified in the analysis. Theme 1: Significant negative impact.* The first theme addressed the significant negative consequences of disruptions for the government sector because of a lack of business continuity planning. An

implication of theme 1 was the acknowledgment of the possible existence of third-party agreements, manual workarounds, systemic redundancies, back-ups, and transfer of risk with insurance companies (Afedzie & McEntire, 2010). However, government agencies have the mandate to continue to provide services to the public, whether or not there is a disruption (Goudsmit, 2012; Klein, 2012). The government sector cares about the implications of disruptions, especially the possible impact on people, property, and the overall monetary loss. The emergence of theme 1 indicated that the government sector might find it difficult to continue to provide services to the public should a disruption occurs, if there was no adequately developed and implemented business continuity plan (DHS, 2013). Additionally, government agencies deal with confidential and sensitive information that could be compromised if business continuity risks were not evaluated properly and assessed. Therefore, without the proper expertise in business continuity planning management might not adequately evaluate and assess the overall risks affecting a government agency; leaving the organization vulnerable if an event occurs (Rosenberg, 2014; Verchick & Hall, 2011).

**Theme 2: Obstacles.** Elements or lack of elements that get in the way of dealing with disruptions successfully. The theme 2 implies that there is a lack of commitment, views that unforeseen issues will never happen, lack of better communication, and unqualified persons being entrusted with dealing with disruptions (Jahangiri et al., 2011). Theme 2 further indicated that key stakeholders and process owners did not consider business continuity of high importance in relation to the overall mission of the organization. Additionally, managements of the government sector are leery about the input of the internal auditor during business continuity planning owing to the threat to



independence, knowledge gaps, or a lack of value being provided by the internal auditor. Theme 2 also implied that involving the internal auditor might negatively affect productivity because of the perception auditors are always looking for mistakes that could warrant a future audit by the internal auditor. Finally, theme 2 also indicated that management's lack of the awareness of the internal auditor's roles in the government could necessitate excluding them in business continuity planning. The implication of theme 2 was that some government agencies seemed to fail to properly perform a full examination of possible issues or threats to business continuity. Therefore, they were unable to assess viable mitigation strategies. Additionally, business continuity was rarely tested in the government sector, and there was a lack of action plans and a lack of resources to properly plan business continuity or action plans (Heller, 2012). Another implication of theme 2 was the failure to develop and implement a business continuity plan (Jarvelainen, 2012). Additionally, the information used in business continuity planning lacked currency.

**Theme 3: Major roles.** Major roles are the reasons for or not involving the internal auditor in the business continuity planning. In theme 3, the importance of the internal auditor in business continuity planning was identified. The internal auditor has a broader and independent understanding of the organization and could provide invaluable insight into areas that are at risk (Kusumasari et al., 2010; Haque et al., 2012). The internal auditor understands risks that might be neglected by management and are in a position to serve in an advisory capacity in the development and implementation of business continuity planning. The implications of this study included providing valuable insights to management, policymakers, and the internal auditor about the perceived roles

of the internal auditor in business continuity planning in the government sector and how to utilize his or her expertise while ensuring independence and objectivity owing to their experience in risk identification and assessment of risks. The participation of the internal auditor would provide reasonable assurance that the business continuity planning process was adequate. Owing to their enterprise-wide risk perspective, internal auditors are positioned to inform those charged with governance regarding the government entity's critical systems and the protection in place (Dickins & Daughterty, 2012; Kotb, Sangster, & Henderson, 2014).

***Theme 4: Areas to be excluded from the internal auditor.*** If internal auditors should be involved in business continuity planning, the areas they should be excluded. Theme 2 implied that internal auditors should be involved in business continuity planning, but they should only participate in an advisory capacity. The implication was that when involvement was in an advisory capacity, the internal auditor would be objective. Additionally, they would be in a position to validate the information provided by various departments of the government sector (Jones, 2015). They accomplish this by identifying key business risks and control gaps, conducting audits when deemed necessary, and serving in an advisory capacity in identifying priorities that affect the government sector (Dickins & Daughterty, 2012; Yoon, Young, & Abe, 2012).

The areas that should be excluded from the internal auditors' participation would include the update and maintenance of the business continuity plan since those are considered management functions (Rosenberg, 2014). Additionally, internal auditors should be excluded from disaster recovery and recovery strategy since they are considered management functions. The implication was that the internal auditor would

be in a position to provide decisive consulting roles in areas that promote efficiency and effectiveness of the business continuity process and help diffuse intra-agency competing interests.

***Theme 5: Internal auditor's independence.*** The reaction of those charged with governance and the necessary safeguards to mitigate the potential impairment of the independence of the internal auditor regarding participation in business continuity planning. Theme 5 implied that the independence of the internal auditor would not be impaired for participating in business continuity planning, but there could be a threat to independence depending on roles of the internal auditor in the process. The implication of theme 5 was that the independence of the internal auditor would not be impaired if the necessary safeguards were put in place by the government sector. These safeguards would include an understanding up front with the management of the government sector outlining the roles of the internal auditor as a consultant, not as someone making management decisions for the organization (Jalba, 2013; Kanellou & Spathis, 2011)

Theme 5 also implied that reactions of those charged with governance could be negative or positive, depending on their understanding of the roles of the internal auditor in business continuity planning within the government sector. As a result, it would be the duty of the internal auditor to explain to management and those charged with governance why the internal auditor should play an active role in business continuity planning within the government sector (Zaman & Sarens, 2013). An implication of theme 5 is that the acceptance of the internal auditor's roles in business continuity planning in the government sector might depend on the internal auditor's ability to convince those

charged with governance that there would be a greater level of assurance in the process owing to the internal auditor's independent assessment and reporting of the process.

**Connection to current literature.** The study expanded the current knowledge of business continuity planning and explored the roles of the internal auditor in business continuity planning in the government sector. Current literature indicated some similarities with the current study in terms of the need for the government sector to implement certain measures to ensure mitigation of disasters and other disruptions.

Current literature supported the importance of business continuity planning to ensure that the government sector is ready to respond to a service disruption or emergency. Additionally, the negative effects of a service disruption or disaster can be significant to the government sector, which might include casualties or even death, negative public perception, property damage, and monetary loss (Day et al., 2012; Haddow et al., 2011). Therefore, when proper skills and knowledge are not used to ensure continuity of business, there is the risk of unsuccessful response to a disaster, and potentially significant losses (Haque et al., 2012; Kusumasari et al., 2010).

Findings from the current study also indicated that the government sector does not consider risks that could impede the government sector's ability to mitigate the impact of disruptions successfully. This assertion contrasts with past research which showed that the government considers different types of risks. Additionally, sometimes staff are not adequately trained on what to do in the event of an emergency (Chen & Lee, 2012).

Current literature focused on the risks facing organizations today. For example, there were risks related to natural disasters such as wind, hail tornadoes, and lightning (Goudsmit, 2012). There were past findings on the need for public asset managers to

mitigate and prepare for future, business continuity planning management in local governments, an exploration on business continuity planning in Michigan small businesses, how to ensure continuity of business in general small and medium businesses, and on education technology (Botha & von Solms, 2004; Lasecki, 2009; Mekdeci, 2011; Smit, 2005; Warren, 2010).

Current literature supported the findings in the current study which included developing and implementing a business continuity plan to mitigate potential loss through the identification, prioritization, and safeguarding of critical assets of the business, not only information technology (Hoong & Marthandan, 2014). Additionally, there were studies supporting the findings in the current study that internal auditors understand and have a broader view of potential risks affecting the organization and the potential impact of any loss (Schneider et al., 2012; Stefaniak et al., 2012). Business continuity is still an emerging concept (Pelfrey & Kelley, 2013). There was no sufficient past literature on the perceived roles of the internal auditor in business continuity planning within the government sector.

Current literature recognized the expertise of the internal audit identifying and prioritizing risk, but there was no sufficient work on the perceived roles of the internal auditor in business continuity planning within the government sector (Schneider et al., 2012; Stefaniak et al., 2012).

## **Recommendations**

**Practical applications.** The five themes supported the recommendations for practice and future research. The findings are relevant to internal auditors, management, and policy makers in the government sector. They can use the information from this

research to gain an adequate understanding of the perceived roles of the internal auditor in the government sector and how to safeguard against the impairment of independence and objectivity. The research findings can assist in possibly mitigating the significant negative impact of disruptions, addressing the obstacles that get in the way of implementing sound business continuity planning, understanding the major roles internal auditors can play in business continuity planning and areas that should be excluded, and the importance of safeguarding the independence of the internal auditor. Additionally, this research provides insight for those charged with governance to ensure the endorsement of the participation of the internal auditor in the business continuity planning in the government sector. Data collected from internal auditors provided insights about how to involve the internal auditor in business continuity planning without compromising objectivity and independence.

There were several recommendations that emerged from this study regarding business continuity planning in the government sector and how the involvement of the internal auditor could aid in mitigating disruptions. The following recommendations arose from the five themes that emerged from this study: (a) understanding the negative impact of disruptions, (2) exploring the obstacles that could prevent implementing business continuity planning and develop mitigation strategies, (c) soliciting the expertise of the internal auditor to ensure all agency-wide risks are considered, (d) excluding the internal auditor from participating in areas that pose significant conflicts, and (e) clarifying the roles of the internal auditor in the organization and getting the support of management and those charged with governance to embrace those roles. These recommendations align with the overarching research question.

It is important to understand the negative impact of disruptions in the government sector. It is somewhat comforting to acknowledge the existence of third-party arrangements, manual workarounds, systemic redundancies, back-ups, and transfer of risk with insurance policies (Afedzie & McEntire, 2010). However, government agencies are expected to continue providing services to the public, whether or not there is a disruption. When business continuity planning is not properly developed and implemented by the government sector, sensitive and confidential data could be compromised or lost. Additionally, a disruption could negatively impact the automated environment, health, and safety of the public. As a result, there might not be viable options to mitigate a disruption if no business continuity planning existed. Also, the government is always concerned about the possible impact on its resources, which includes people, equipment, operating systems, and facilities (Goudsmit, 2012; Klein, 2012).

When business continuity planning is being implemented without the involvement of the internal auditor, chances are significant risks may not be considered. Additionally, when pertinent risks are not considered during the business continuity process, the effect could be catastrophic (DHS, 2013). As a result, management should make concerted efforts to ensure proper mitigation of any potential disruption. One of the crucial ways of accomplishing this is through the implementation of business continuity planning. A good business continuity planning requires the involvement of the right personnel which includes those knowledgeable in organization-wide risk assessment and analysis and the buy-in of those charged with governance.

Again, mitigation of disruptions is very crucial to the government sector because they continue to protect the interest of the public. Regrettably, some government agencies fail properly to perform a full analysis of potential disruptions or risks, thereby defaulting to being unable to assess immediate mitigation strategies. A part of the reasons includes the use of outdated information and data that are not aligned with the objectives and mission of the government agency. Additionally, oftentimes, there is the belief that disruptions will never happen, and some do not see the need for business continuity planning owing to the third-party transfer of risk. Additionally, the right individuals are not assigned to develop and implement a business continuity plan. As a result, all pertinent risks are not usually considered. Some government agencies perceive internal auditors as a hindrance to planning because of their roles in the organization.

The right individuals should be involved in business continuity planning. The personnel should be trained on how to identify and respond to a disruption. Also, the business continuity plan must be tested and updated periodically. Additionally, there should be training focusing on risks affecting the government sector, the probability of occurrence, the potential impact of those risks, strategies for mitigating them, and selecting the right strategy.

The third recommendation pertains to the roles of the internal auditor in business continuity planning. Oftentimes, management of the government sector might neglect certain risks that could have potential negative impact on the organization. The impact might include delay or shut down of services which ultimately could affect the health and safety, facilities, and even employees. Fortunately, the government internal auditor has an in-depth understanding of the risks facing the organization as a whole. This



understanding is on account of their roles in the organization as experts in risk assessment.

Most of the areas within the government sector probably had been audited in the past by the internal auditors. As a result, they are in a position to provide an objective insight into areas within the organization that are susceptible to risk. They can review risk assessment and analysis conducted by management and other personnel of the government sector for the adequacy and appropriateness. They can assist with business impact analysis and possibly audit the business continuity plan to ensure relevancy to the government sector.

The review of the business continuity plan allows the internal auditor to identify weaknesses that could be rectified prior to a disruption materializing. The internal auditor also could be the eyes and ears of those charged with governance in terms of the comprehensiveness of the business continuity plan. Finally, there should be training on the roles of the internal auditor. The internal audit charter should be reviewed and updated periodically to ensure the roles of the internal auditors are fully defined and that their expertise is maximized by the government sector.

The fourth and fifth recommendations pertain to the exclusion of the internal auditor from participating in areas that pose significant conflicts, clarifying the roles of the internal auditor in the organization, and obtaining the support of management and those charged with governance to embrace those roles. Although internal auditors are considered experts in risk assessment and mitigation due to their overall knowledge of the organization, their participation in business continuity planning in the government sector should be in an advisory capacity. In essence, they should not be participating in

management functions. Non-participation in management functions would ensure objectivity in the internal auditor's roles. For example, the internal auditor should not be participating in the update and maintenance of the business continuity plan because those are considered management functions.

Additionally, disaster recovery should be performed by management and staff rather than the internal auditor because they are considered management functions. Nevertheless, the internal auditor should be involved in analysis and testing of the business continuity plan so as to provide objective insight to management and those charged with governance about the results. Although internal auditors might not be directly involved in the business impact analysis since it is a management, they should provide essential insight to management and staff to ensure the necessary risks are considered. Consideration of necessary risks is also essential in diffusing intra-agency competing interests during the initiation of business continuity planning. Although the internal auditor's participation in business continuity planning is essential in business continuity planning, there could be a threat to the independence of the internal auditor if their role is not properly defined. To mitigate any threat, there should be safeguards in place. First, there should be an understanding with management and those charged with governance in the government sector delineating the roles of the internal auditors in the organization and their levels of participation in business continuity planning. They should not be making decisions for management but should be considered as consultants. An example of such agreement should be in the form of a Memorandum of Understanding or a Statement of Work. This agreement will clarify the roles of the internal auditor with respect to business continuity planning. Therefore, the internal

auditor should not be the owner of the business continuity plan; and as a result, he or she cannot participate in determining priorities within the organization.

The reactions of those charged with governance could be positive or negative in terms of the internal auditor's participation in business continuity planning. However, it is the duty of the internal auditor to clarify to management and those charged with governance the reasons for the internal auditor's participation (Muqattash, 2011; Aikins, 2012). An alternative method of clarifying might include referring them to the Internal Auditor Charter. The charter spells out the responsibilities of the internal auditor in the organization. With a full understanding of the roles of the internal auditor, those charged would embrace the independence and objectivity of the internal auditor and should welcome such role (Dickins & Daughterty, 2012; Elmore, 2013; Kotb, Sangster, & Henderson, 2014; de Zwaan et al., 2011; ).

. **Future research.** Three recommendations are being considered for future research. The first is to determine whether the internal auditor should play a role in maintenance and update of the business continuity plan. The public expects the government to ensure continuity of operations. The lack of an updated business continuity plan could pose a significant risk to the organization when the documents become outdated and can not be invoked during a disruption (Campbell, 2013; McGuire & Schneck, 2010). These risks could be mitigated by employing properly designed business continuity planning that considered the business impact analysis, security risks, recovery alternatives, implementation, and maintenance, utilizing the right personnel. These individuals would determine how and when to update the business continuity plan. The updated business continuity plan should continue to align with the objectives of the

organization to ensure swift mitigation of any disaster or disruption. Future research needs to explore whether it is necessary for internal auditor to play any role in the update and maintenance of the business continuity plan, especially as someone who broadly understands the risks that are pertinent to the organization (Amaratunga, 2014; A. C. K. Lee, Booth, Challen, Gardois, & Goodacre, 2014; McGrady & Blanke, 2014).

The second recommendation is to determine why organizations would be reluctant to test their business continuity plans periodically. Governments must be genuine and reliable in providing services for the public, especially when mitigating disruptions (Koronis & Ponis, 2012). The Internet has provided efficiency and effectiveness in all aspects of the world. Additionally, the number of connections and data exchange has increased (Ghezzi et al., 2013). Additionally, technology has made the world one interconnected marketplace. Therefore, there are questions on how to manage and govern it (De Turck et al., 2012).

Organizations are steadily transitioning from stand-alone word processing and paper filing to server-based systems (Friedman, 2014). These systems make it easier to access documents remotely and obtain real-time information. As more and more catastrophic events occur, organizations and the public as a whole are concerned about business continuity. When a crisis is not properly mitigated, there could be a temporary disconnection with the public or other users of services or even permanent disruption of business relations (Koronis & Ponis, 2012). The public expectations have caused some regulatory agency personnel to begin thinking seriously about business continuity planning (Jones, 2011). Consequently, it is necessary to develop and implement business continuity planning to ensure mitigation of disruptions. The business continuity plan

should be tested periodically to ensure management can truly mitigate disruptions whenever they occur. Oftentimes, organizations are reluctant to test their business continuity plans (Abramson et al., 2015; Amaratunga, 2014; McGrady & Blanke, 2014). Future research needs to determine why some organizations are reluctant to test their business continuity plans.

The third recommendation is to determine the roles of the internal auditor in business impact analysis during the development of a business continuity plan. Business impact analysis is considered one of the foremost steps organizations follow during the development of the business continuity plan (Kent, 2011). A governmental agency that is developing a business continuity plan identifies events that could negatively impact operations, especially financial information (Bajgoric, 2014; Nicoll & Owens, 2013). Therefore, to complete this aspect of the business continuity plan process, there should be an adequate understanding of the government sector's operations, its key processes, and technology platform used by the government agency. Additionally, there should be consideration of cost, downtime, and recovery of data (Davison, 2014). The overall goal should be to mitigate disruptions at minimal costs (Davison, 2014). Since the internal auditor understands the operations of the entity, future research should consider exploring whether the internal auditor should play a role in business impact analysis.

### **Conclusions**

This qualitative case study explored the perceived roles of the internal auditor in business continuity planning in the government sector. This chapter contains a discussion of the findings emerging from the research and the implications of the roles of the internal auditor in business continuity planning. Additionally, there are

recommendations for practical applications and suggestions for future research. The conclusions arising from this research are presented.

The risks could be severe when a government entity fails to implement measures to ensure continuity of operations. Such risks would include the inability to respond to an emergency and the inefficient use of limited resources. The government sector is worried about people, property damage, and monetary loss, but findings of the research indicated that government entities are not giving enough attention to confidential and sensitive information. Sometimes the government sector would not consider risks that could impede their ability to mitigate disruptions. As a result, they could potentially expose their organizations to significant losses.

Findings from the current study also indicated that the government sector did not consider risks that could hinder the entity from successful mitigation of disruptions because preference was given to other pressing issues affecting the government sector. Additionally, management of the government sector cites the lack of adequate resources as the reason for not paying greater attention to business continuity planning. Surprisingly, while some governmental entities that had business continuity plans rarely tested them, there were those who believed a disruption would never occur. There was a lack of commitment or communication, training about mitigating disruptions, and inept personnel being assigned to deal with disruptions, and business impact analysis data were accurate and not aligned to the government sector's mission and objectives.

The findings also indicated that some members of organizations would prefer non-participation of the internal auditor in business continuity planning. This preference was because of the perceived threat to the internal auditor's independence. Some

reasoned that the internal auditor's participation would be useless because they would not provide value because of a lack of knowledge. As a result, the internal auditor would be a hindrance in business continuity planning. Additionally, the internal auditor might not have a good rapport with some members of the organization just because they are auditors who might be looking for deficiencies that necessitate conducting future audits of different departments. Another issue was that, sometimes, management might not be cognizant of the roles of the internal auditor in the organization, and as a result, they would be reluctant to get them involved in business continuity planning.

Internal auditors should be involved in the business continuity planning in the government sector because of their knowledge of the entity and insight about risks affecting the organization. There might be a threat to the internal auditor's independence owing to participation in business continuity planning and a subsequent audit of the process by the internal auditor. To mitigate such a threat, the organization and internal auditor should implement safeguards. Such safeguards might include having a written understanding with management at the outset of the engagement delineating the roles the internal auditor as an advisor and not as an individual who would be participating in management decisions. Additionally, the documented understanding would assure management and those charged with governance of the internal auditor's objectivity in the business continuity planning process.

Internal auditors' perceived roles in business continuity planning in the government sector would include the identification of risks and the approach for combating those risks, objective prioritization of critical processes, familiarization, and categorization of the limited resources needed for those services, and evaluation of

recovery strategies to ensure properly developed and implemented business continuity planning. The overall objective would be to mitigate disruptions and continue to meet the public mandate for the government.



## References

- Abbass, D. A., & Aleqab, M. M. (2013). Internal auditors' characteristics and audit fees: Evidence from Egyptian firms. *International Business Research*, 6(4), 67-80. <http://dx.doi.org/10.5539/ibr.v6n4p67>
- Abbott, L. J., Daugherty, B., Parker, S., & Peters, G. F. (2016). Internal audit quality and financial reporting quality: The joint importance of independence and competence. *Journal of Accounting Research*, 54, 3-40. <http://dx.doi.org/10.1111/1475-679X.12099>
- Abramson, D. M., Grattan, L. M., Mayer, B., Colten, C. E., Arosemena, F. A., Bedimorung, A., & Lichtveld, M. (2015). The resilience activation framework: A conceptual model of how access to social resources promotes adaptation and rapid recovery in post-disaster settings. *The Journal of Behavioral Health Services & Research*, 42, 42-57. <http://dx.doi.org/10.1007/s11414-014-9410-2>
- Adams, L. M. (2008). Comprehensive vulnerability management: The road to effective disaster planning with the community. *Journal of Theory Construction & Testing*, 12(1), 25-27. Retrieved from <http://tuckerpub.com/jtct.htm>
- Adini, B., Laor, D., Cohen, R., & Israeli, A. (2012). Decision to evacuate a hospital during an emergency: The safe way or the leader's way? *Journal of Public Health Policy*, 33, 257-268. <http://dx.doi.org/10.1057/jphp.2012.2>
- Afedzie, R., & McEntire, D. A. (2010). Rethinking disasters by design. *Disaster Prevention and Management*, 19, 290-295. <http://dx.doi.org/10.1108/09653561011022135>
- Aikins, S. K. (2011). An examination of government internal audits' role in improving financial performance. *Public Finance and Management*, 11, 306-337. Retrieved from <https://www.scribd.com/document/188244398/AUDITS-ROLE-IN-IMPROVING-FINANCIAL-performance>
- Aikins, S. K. (2012). Determinants of auditee adoption of audit recommendations: Local government auditors' perspectives. *Journal of Public Budgeting, Accounting & Financial Management*, 24, 195-220. Retrieved from [http://pracademics.com/attachments/article/847/Article%201\\_Aikins.pdf](http://pracademics.com/attachments/article/847/Article%201_Aikins.pdf)
- Akkiraju, R., Bhattacharjya, D., & Gupta, S. (2012). Towards effective business process availability management. *Journal of Service Science Research*, 4, 319-351. <http://dx.doi.org/10.1007/s12927-012-0013-2>
- Alam, I. (2005). Fieldwork and data collection in qualitative marketing research. *Qualitative Market Research*, 8(1), 97-112. <http://dx.doi.org/10.1108/13522750510575462>

- Aleem, A., & Christopher, R. S. (2013). Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime*, 20(1), 6-24. <http://dx.doi.org/10.1108/13590791311287337>
- Allen, L. E. (2008). Where good ERP implementations go bad: A case for continuity. *Business Process Management Journal*, 14, 327-337. <http://dx.doi.org/10.1108/14637150810876661>
- Al-Matari, E. M., Al-Swidi, A. K., & Fadzil, F. H. B. (2014). The effect of the internal audit and firm performance: A proposed research framework. *International Review of Management and Marketing*, 4(1), 34-41. Retrieved from <http://www.econjournals.com/index.php/irmm/article/viewFile/669/pdf>
- Amancei, C. (2011). Practical methods for information security risk management. *Informatica Economica*, 15(1), 151-159. Retrieved from <http://www.revistaie.ase.ro/content/57/13%20-%20Amancei.pdf>
- Amaratunga, C. A. (2014). Building community disaster resilience through a virtual community of practice (VCOP). *International Journal of Disaster Resilience in the Built Environment*, 5, 66-78. <http://dx.doi.org/10.1108/ijdrbe-05-2012-0012>
- American Psychological Association (APA). (2010). *Ethical principles of psychologists and code of conduct: 2010 amendments*. Retrieved from <http://www.apa.org/ethics/code/>
- Anderson, U. L, Christ, M. H., Johnstone, K. M., & Rittenberg, L. A. (2012). A post-SOX examination of factors associated with the size of internal audit functions. *Accounting Horizons*, 26(12), 167-191. <http://dx.doi.org/10.2308/acch-50115>
- Arwood, T., & Panicker, S. (2011). *Assessing risk in social and behavioral sciences*. Retrieved from <https://www.citiprogram.org/>
- Asgary, A., & Mousavi-Jahromi, Y. (2011). Power outage, business continuity and businesses' choices of power outage mitigation measures. *American Journal of Economics and Business Administration*, 3, 312-320. <http://dx.doi.org/10.3844/ajebasp.2011.307.315>
- Ayalon, Y. (2011). Ottoman urban privacy in light of disaster recovery. *International Journal of Middle East Studies*, 43, 513-528. <http://dx.doi.org/10.1017/S002074381100064X>
- Badara, M. S., & Saidin, S. Z. (2013). The journal so far on internal audit effectiveness: A calling for expansion. *International Journal of Academic Research in Accounting, Financial, and Management Sciences*, 3, 340-351. <http://dx.doi.org/10.6007/ajarafms/v3-i3/223>

- Baird, J. E., Zelin, R. C., II, & Booker, Q. E. (2012). Is there a "digital divide" in the provision of e-government services at the county level in the United States? *Journal of Legal, Ethical and Regulatory Issues*, 15(1), 93-104. Retrieved from <http://www.alliedacademies.org/legal-ethical-and-regulatory-issues/>
- Bajgoric, N. (2014). Business continuity management: A systemic framework for implementation. *Kybernetes*, 43, 156-177. <http://dx.doi.org/10.1108/K-11-2013-0252>
- Baker, N. (2012). Enterprise business continuity. *Internal Auditor: Journal of the Institute of Internal Auditors*, 69(3), 36-40. Retrieved from <https://na.theiia.org/periodicals/Pages/Internal-Auditor-Magazine.aspx>
- Barnett-Page, E., & Thomas, J. (2009). Methods for the synthesis of qualitative research: a critical review. *BMC Medical Research Methodology*, 9, Art. 59. <http://dx.doi.org/10.1186/1471-2288-9-59>
- Bayrak, T. (2009). Identifying requirements for a disaster. *The Daily Post*, 18(2), 23-26. <http://dx.doi.org/10.1108/09653560910953171>
- Beets, S. D. (2011). Critical events in the ethics of U.S. corporation history. *Journal of Business Ethics*, 102, 193-219. <http://dx.doi.org/10.1007/s10551-011-0805-1>
- Beggan, D. M. (2011). Disaster recovery consideration for academic institutions. *Disaster Prevention and Management*, 20, 413-422. <http://dx.doi.org/10.1108/09653561111161734>
- Ben-Shahar, O., & Logue, K. D. (2013). Outsourcing regulation: How insurance reduces moral hazard. *Social Science Research Network Electronic Journal*. 111(2). <http://dx.doi.org/10.2139/ssrn.2038105>
- Berenfeld, M. (2007). Disaster preparedness: How to develop a business continuity plan. *Infotech Update*, 16(5), 5-6. Retrieved from <https://rangrez.wordpress.com/2009/08/11/disaster-preparedness-how-to-develop-a-business-continuity-plan/>
- Biedrzycki, P., & Koltun, R. (2012). Integration of social determinants of community preparedness and resiliency in 21st century emergency management planning. *Homeland Security Affairs*, 8(1), 1-8. Retrieved from <http://www.hsaj.org>
- Born, P. H., & Klimaszewski-Blettner, B. (2013). Should I stay or should I go? *Journal of Risk and Insurance*, 80(1), 1-36. <http://dx.doi.org/10.1111/j.1539-6975.2012.01477.x>
- Botha, J., & von Solms, R. (2004). A cyclical approach to business continuity planning. *Information Management and Computer Security*, 12, 328-337. <http://dx.doi.org/10.1108/09685220410553541>

- Bowyer, D., & Davis, G. (2012). How to acquire aircraft? A grounded theory approach to case study research. *Qualitative Research in Accounting and Management*, 9, 363-397. <http://dx.doi.org/10.1108/11766091211282670>
- Bryman, A., & Bell, E. (2011). *Business research methods* (3rd ed.). New York, NY: Oxford University Press Inc.
- Burnaby, P. A., & Hass, S. (2011). Internal auditing in the Americas. *Managerial Auditing Journal*, 26, 734-756. <http://dx.doi.org/10.1108/02686901111161359>
- Burnaby, P. A., Hass, S., & Abdolmohammadi, M. J (2009). A global summary of internal auditing common body of knowledge. *Internal Auditing*, 24(1), 13-26. <http://www.theiaa.org>
- Busch, N. E., & Givens, A. D. (2013). Achieving resilience in disaster management: The role of public-private partnerships. *Journal of Strategic Security*, 6(2), 1-19. <http://dx.doi.org/10.5038/1944-0472.6.2.1>
- Calderon, T. G., (2003). Assurance and recovery cost optimization in business continuity planning. *Internal Auditing*, 18(2), 20-29. Retrieved from <http://www.iaa.org.au/technicalresources/internalAuditorMagazine.aspx>
- Camara, S., Crossler, R., Midha, V., & Wallace, L. (2011). Teaching case: Bank solutions disaster recovery and business continuity: A case study for business students. *Journal of Information Systems Education*, 22, 117-122. Retrieved from <http://www.cis.gsu.edu/rbaskerville/cis8630/cases/banksolutions.pdf>
- Campbell, A. (2013). Top 10: Operational risks 2013. *Operational Risk & Regulation*, 13(12), 32-39. Retrieved from <http://www.risk.net/operational-risk.../top-10-operational-risks-for-2013>
- Carrington, C.M. (2010). *Avoiding disaster before it strikes*. Retrieved from <http://www.multichannel.com/content/avoiding-disaster-it-strikes>
- Carson, J. M., McCullough, K., & Pooser, D. M. (2013). Deciding whether to invest in mitigation measures: Evidence from Florida. *Journal of risk and insurance*, 80, 308-327. <http://dx.doi.org/10.1111/j.1539-6975.2012.01484.x>
- Cascardo, D. (2012). Preparing your practice for any emergency scenario: Your practice continuity plan. *The Journal of Medical Practice Management*, 27, 199-202. Retrieved from [https://www.greenbranch.com/store/index.cfm/product/4\\_31/the-journal-of-medical-practice-management.cfm](https://www.greenbranch.com/store/index.cfm/product/4_31/the-journal-of-medical-practice-management.cfm)
- Cascardo, D. (2013). Learning to live with volatility: Preparing for business continuity and recovery following a disaster. *The Journal of Medical Practice Management*, 28, 282-285. Retrieved from <http://www.biomedsearch.com/nih/Learning-to-live-with.../23767119.html>

- Cereola, S. J., & Cereola, R. J. (2011). Breach of data at TJX: An instructional case used to study COSO and COBIT, with a focus on computer controls, data security, and privacy legislation. *Issues in Accounting Education*, 26(3), 521-545. <http://dx.doi.org/10.2308/iace-50031>
- Chambers, A. D. (2014). New guidance on internal audit - an analysis and appraisal of recent developments. *Managerial Auditing Journal*, 29, 196-218. <http://dx.doi.org/10.1108/maj-08-2013-0925>
- Chamlee-Wright, E. (2010). Expectations of response to disaster. *Public Choice*, 144(1), 253-274. <http://dx.doi.org/10.1007/s11127-009-9516-x>
- Chandra, A., Williams, M., & Tang, J. (2013). Getting actionable about community resilience: The Los Angeles county community disaster resilience project. *American Journal of Public Health*, 103, 1181-1189. Retrieved from <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3682620/>
- Chang, S.-I., Huang, S.-M., Roan, J., Chang, I.-C., Ying, P.-J. (2014). Developing risk management assessment framework for public administration in Taiwan. *Risk Management*, 16, 164-194. <http://dx.doi.org/10.1057/rm.2014.9>
- Chang, Y., Wilkinson, S., Potangaroa, R., & Seville, E. (2012). Managing resources in disaster recovery projects. *Engineering, Construction and Architectural Management*, 19, 557-580. <http://dx.doi.org/10.1108/09699981211259621>
- Chen, C.-Y., & Lee, W.-C. (2012). Damages to school infrastructure and development to disaster prevention education strategy after typhoon Morakot in Taiwan. *Disaster Prevention and Management*, 21, 541-555. <http://dx.doi.org/10.1108/09653561211278680>
- Christopher, C., Sarens, G., & Leung, P. (2009). A critical analysis of the independence of the internal audit function: evidence from Australia. *Accounting, Auditing & Accountability Journal*, 22, 200-220. <http://dx.doi.org/10.1108/09513570910933942>
- Coles, J., & Zhuang, J. (2011). Decisions in disaster recovery operations: A game theoretic perspective on organization cooperation. *Journal of Homeland Security and Emergency Management*, 8(1), 1-14. doi:10.2202/1547-7355.1772
- Converse, M. (2012). Philosophy of phenomenology: How understanding aids research. *Nurse Researcher*, 20(1), 28-32. Retrieved from <http://dx.doi.org/10.7748/nr2012.09.20.1.28.c9305>
- Cox, R. S., & Perry, K. E. (2011). Like a fish out of water: Reconsidering disaster recovery and the role of place and social capital in community disaster resilience. *American Journal of Community Psychology*, 48, 395-411. <http://dx.doi.org/10.1007/s10464-011-9427-0>

- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage.
- Crowe, S., Creswell, K., Robertson, A., Huby, G., Avery, A. & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, 11(100). <http://dx.doi.org/10.1186/1471-2288-11-100>
- Darrough, M.N. (2010). The FCPA and the OECD convention: Some lessons from the U.S. experience. *Journal of Business Ethics*, 93, 255-276. <http://dx.doi.org/10.1007/s10551-009-0219-5>
- Davison, C. B. (2014). Selected leadership demographics as predictors of continuity planning. *Disaster Prevention and Management*, 23, 243-251. <http://dx.doi.org/10.1108/dpm-08-2013-0140>
- Day, J. M., Melnyk, S. A., Larson, P. D., Davis, E. W., & Whybark, D. C. (2012). Humanitarian and disaster relieve supply chains: A matter of life and death. *Journal of Supply Chain Management*, 48(2), 21-36. <http://dx.doi.org/10.1111/j.1745-493X.2012.03267.x>
- Department of Homeland (DHS). (2006). *Nationwide plan review phase 2 report*. Retrieved from [http://www.dhs.gov/xlibrary/assets/Prep\\_NationwidePlanReview.pdf](http://www.dhs.gov/xlibrary/assets/Prep_NationwidePlanReview.pdf)
- Department of Homeland (DHS). (2008). *National response framework*. Retrieved from <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>
- Department of Homeland (DHS). (2011a). *Implementing 9/11 commission recommendations*. Retrieved from <http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf>
- Department of Homeland (DHS). (2011b). *National preparedness goal*. Retrieved from [http://www.fema.gov/media-library-data/20130726-1828-25045-9470/national\\_preparedness\\_goal\\_2011.pdf](http://www.fema.gov/media-library-data/20130726-1828-25045-9470/national_preparedness_goal_2011.pdf)
- Department of Homeland (DHS). (2013a). *Preparedness planning for your business*. Retrieved from <http://www.ready.gov/business>
- Department of Homeland (DHS). (2015). *Introduction to continuity of operations*. Retrieved from <https://training.fema.gov/is/courseoverview.aspx?code=IS-547.a>
- Desai, R., & Roberts, R. W. (2013). Deficiencies in the code of conduct: The AICPA rhetoric surrounding the tax return preparation outsourcing disclosure rules. *Journal of Business Ethics*, 114, 457-471. <http://dx.doi.org/10.1007/s10551-012-1329-z>

- De Smet, H., Lagadec, P., & Leysen, J. (2012). Disasters out of the box: A new ballgame? *Journal of Contingencies and Crisis Management*, 20(3), 138-148. doi:10.1111/j.1468-5973.2012.00666.x
- De Turck, F., Kiriha, Y., & Hong, J. W.-K. (2012). Management of the future internet: Status and challenges. *Journal of Network and Systems Management*, 20, 616-624. <http://dx.doi.org/10.1007/s10922-012-9245-1>
- Deverell, E. (2012). Investigating the roots of crisis management studies and outlining future trajectories for the field. *Journal of Homeland Security and Emergency Management*, 9(1), 1-18. doi:10.1515/1547-7355.24
- de Zwaan, L., Stewart, J., & Subramaniam, N. (2011). Internal audit involvement in enterprise risk management. *Managerial Auditing Journal*, 26, 586-604. <http://dx.doi.org/10.1108/02686901111151323>
- Dickey, P. K., Schwagel, T., & White, S. (2006). In the event of disaster, *Internal Auditor: Journal of the Institute of Internal Auditors*, 63, 89-93. Retrieved from <https://na.theiia.org/periodicals/Pages/Internal-Auditor-Magazine.aspx>
- Dickins, D., & Daughterty, B. (2012). Should those charged with corporate governance care about auditor offshoring? *International Journal of Disclosure and Governance*, 9(1), 52-61. <http://dx.doi.org/10.1057/jdg.2011.11>
- Dickins, D., & Reisch, J. T. (2012). Enhancing auditors' ability to identify opportunities to commit fraud: Instructional resource cases. *Issues in Accounting Education*, 27, 1153-1169. <http://dx.doi.org/10.2308/iace-50178>
- Ditch, R. L. (2014). [Review of the book, *The business of counterterrorism. Public-private partnerships in homeland security*, by N. E. Busch & A. D. Givens]. *Journal of Strategic Security*, 7(3), 100-101. <http://dx.doi.org/10.5038/1944-0472.7.3.8>
- Donahue, D. A., Cunnion, S. O., Balaban, C. D., & Sochats, K. (2012). The all needs approach to emergency response. *Homeland Security Affairs*, 8, Art. 1. Retrieved from <https://www.hsaj.org/articles/204>
- Dowling, M., & Cooney, A. (2012). Research approaches related to phenomenology: Negotiating a complex landscape. *Nurse Researcher*, 20(2), 21-27. Retrieved from <http://dx.doi.org/10.7748/nr2012.11.20.2.21.c9440>
- D'Onza, G., Selim, G. M., Melville, R., & Allegrini, M. (2015). A study on internal auditor perceptions of the function ability to add value. *International Journal of Auditing*, 19, 182-194. <http://dx.doi.org/10.1111/ijau.12048>

- Drost, E. A. (2011). Validity and reliability in social science research. *Education Research and Perspectives*, 38, 105-124. Retrieved from <http://www.erjournal.net/wp-content/uploads/2012/07/ERP38-1.-Drost-E.-2011.-Validity-and-Reliability-in-Social-Science-Research.pdf>
- Dudin, E. B., & Smetanin, Y. G. (2011). A review of cloud computing. *Scientific and Technical Information Processing*, 38, 280-284. <http://dx.doi.org/10.3103/S0147688211040083>
- The E-Government Act of 2002, Pub. L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101 (2002).
- Elmore, T. P. (2013). The role of internal auditors in creating an ethical culture. *The Journal of Government Financial Management*, 62(2), 48-53. Retrieved from <https://www.agacgfm.org/Resources/Journal-of-Government-Financial-Management.aspx>
- Elo, S., & Kyngas, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1), 107-115. <http://dx.doi.org/10.1111/j.1365-2648.2007.04569.x>
- Epstein, P. D. (2010). Auditor roles in government performance management. *Government Finance Review*, 26(6), 51-55. Retrieved from [gfoa.org/gfr](http://gfoa.org/gfr)
- Erickson, P. A. (2006). *Emergency response planning for corporate and municipal managers* (2nd ed.). Burlington, MA: Butterworth-Heinemann.
- Eriksson, K. (2009). Knowledge transfer between preparedness and emergency response: A case study. *Disaster Prevention and Management*, 18(2), 162-169. doi:10.1108/09653560910953234
- Essers, J. (2012). RE-writing the organization: The ideological deadlock of narrative methodology. *Journal of Organizational Change Management*, 25, 332-351. <http://dx.doi.org/10.1108/09534811211213991>
- Expedited Funds Availability Act, 41 U.S.C. 12 § 229 (1987).
- Faith, K., Jackson, B. A., & Willis, H. (2011). Text analysis of after action reports to support improved emergency response planning. *Journal of Homeland Security and Emergency Management*, 8(1), 1-16. <http://dx.doi.org/10.2202/1547-7355.1900>
- Farber, D. (2011). Symposium introduction: Navigating the intersection of environmental law and disaster law. *Brigham Young University Law Review*, 2011, 1783-1820. Retrieved from <http://digitalcommons.law.byu.edu/lawreview/>
- Farley, T. A., & Weisfuse, I. (2011). Redefining of public health preparedness after 9/11. *The Lancet*, 378, 957-959. [http://dx.doi.org/10.1016/s0140-6736\(11\)60969-0](http://dx.doi.org/10.1016/s0140-6736(11)60969-0)



- Federal Emergency Management Agency (FEMA). (2009). *Handbook for rapid visual screening of buildings to evaluate terrorism risks* (FEMA 455). Retrieved from [http://www.fema.gov/media-library-data/20130726-1457-20490-8140/01\\_fema\\_455\\_cvr\\_frwd\\_ack\\_toc.pdf](http://www.fema.gov/media-library-data/20130726-1457-20490-8140/01_fema_455_cvr_frwd_ack_toc.pdf)
- Federal Emergency Management Agency (FEMA). (2015). *What is Mitigation? Who benefits from it?* Retrieved from <http://www.fema.gov/whobenefitsfromit>
- Finlay, L. (2009). Debating phenomenological research methods. *Phenomenology & Practice*, 3(1), 6-25. Retrieved from [http://www.psyking.net/HTMLobj-3824/Debating\\_Phenomenological\\_Research\\_Methods.pdf](http://www.psyking.net/HTMLobj-3824/Debating_Phenomenological_Research_Methods.pdf)
- Finlayson, K. W., & Dixon, A. (2008). Qualitative meta-synthesis: A guide for the novice. *Nurse Researcher*, 15(2), 59-71. <http://dx.doi.org/10.7748/nr2008.01.15.2.59.c6330>
- Flood Disaster Protection Act of 1973, 42 U.S.C. 4001 et seq. (1973).
- Foreign Corrupt Practices Act, Pub. L. 95-213, 91 Stat. 1494 (1977).
- Four emerging business continuity trends identified in new ISACA White Paper*. (2012, December 27). Retrieved from <http://www.apnnews.com/2012/12/28/four-emerging-business-continuity-trends-identified-in-new-isaca-white-paper/>
- Franck, P., & Sundgren, S. (2012). Determinants of internal governance quality: Evidence from Sweden. *Managerial Auditing Journal*, 27, 639-665. <http://dx.doi.org/10.1108/02686901211246796>
- Friedman, J. (2014, June 23). *Mission-critical business continuity and disaster recovery strategies*. Retrieved from <http://www.propertycasualty360.com/2014/.../mission-critical-business-continuity>
- Garcia, A. (2008, November 7). Business continuity: Best practices. *eWeek*. Retrieved from <http://www.eweek.com/c/a/IT-Management/Business-Continuity-Best-Practices>
- García, L. S., Barbadillo, E. R., & Pérez, M. O. (2012). Audit committee and internal audit and the quality of earnings: Empirical evidence from Spanish companies. *Journal of Management & Governance*, 16, 305-331. <http://dx.doi.org/10.1007/s10997-010-9152-3>
- Gauthier, S. J. (2007). A new vision for public sector audit committees. *Government Finance Review*, 23(2), 10-16. Retrieved from [https://www.alamo.edu/uploadedFiles/District/Employees/Departments/Internal\\_Audit/Files/A-New-Vision-for-Public-Sector-AuditCommittees-GFR\\_apr07.pdf](https://www.alamo.edu/uploadedFiles/District/Employees/Departments/Internal_Audit/Files/A-New-Vision-for-Public-Sector-AuditCommittees-GFR_apr07.pdf)
- Geale, S.K. (2012). The ethics of disaster management. *Disaster Prevention and Management*, 21, 445-462. <http://dx.doi.org/10.1108/09653561211256152>

- Ghezzi, A., Georgiades, M., Reichl, P., Le-Sauze, N., Cairano, C. D., & Managiaracina, R. (2013). Generating innovative interconnection business models for the future internet. *Info : The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*, 15(4), 43-68. <http://dx.doi.org/10.1108/info-12-2012-0054>
- Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. New York, NY: Aldine de Gruyter.
- Glendon, L. (2013). A winning combination: The 3Cs of business continuity. *Journal of Business Continuity & Emergency Planning*, 7(1), 44-55. Retrieved from <http://henrystewart.metapress.com/link.asp?id=n5w44972k7512351>
- Goldberg, E. (2013). Preventing a data breach from becoming a disaster. *Journal of Business Continuity & Emergency Planning*, 6, 295-303. Retrieved from <http://henrystewart.metapress.com/link.asp?id=85163430476442hj>
- Goudsmit, F. (2012). Disaster planning for biotechnology companies. *Journal of Commercial Biotechnology*, 18(3), 58-61. <http://dx.doi.org/10.5912/jcb.529>
- Gourio, F. (2012). Disaster risk and business cycles. *The American Economic Review*, 102, 2734-2766. <http://dx.doi.org/10.1257/aer.102.6.2734>
- Grimaila, M. R., & Badiru, A. (2013). A hybrid dynamic decision making methodology for defensive information technology contingency measure selection in the presence of cyber threats. *Operational Research*, 13, 67-88. <http://dx.doi.org/10.1007/s12351-010-0102-2>
- Grosskopf, K. R. (2010). Disaster preparedness: How to develop a business continuity plan. *International Journal of Disaster Resilience*, 1, 322-335. <http://dx.doi.org/10.1108/17595901011080904>
- Gruiescu, M., Ioanăș, C., & Morega, D. D. (2010). The risk connection of an organization with internal audit. Specific corporate governance practices. *Romanian Economic and Business Review*, 5, 258-270. Retrieved from <http://www.rebe.rau.ro/RePEc/rau/journal/FA10/REBE-FA10-A20.pdf>
- Gunnec, D., & Salman, F. S. (2011). Assessing the reliability and the expected performance of a network under disaster risk. *OR Spectrum*, 33, 499-523. <http://dx.doi.org/10.1007/s00291-011-0250-7>
- Guster, D. C., Lee, O. F., & McCann, B. P. (2012). Outsourcing and replication considerations in disaster recovery planning. *Disaster Prevention and Management*, 21, 172-183. <http://dx.doi.org/10.1108/09653561211219982>
- Guxholli, S., Karapici, V., & Gjinopulli, A. (2012). Corporate governance and audit. *China - USA Business Review*, 11(2) Retrieved from <http://www.davidpublishing.org>

- Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2011). *Introduction to emergency management* (4th ed.). Burlington, MA: Butterworth-Heinemann.
- Hall, D. J., Skipper, J. B., Hazen, B. T., & Sawalha, J. B. (2012). Inter-organizational IT use, cooperative attitude, and inter-organizational collaboration as antecedents to contingency planning effectiveness. *International Journal of Logistics Management*, 23(1), 50-76. <http://dx.doi.org/10.1108/09574091211226920>
- Haque, U., Hashizume, M., Kolivras, K. N., Overgaard, H. J., Das, B., & Yamamoto, T. (2012). Reduced death rates from cyclones in Bangladesh: What more needs to be done? *Bulletin of the World Health Organization*, 90, 150-156. <http://dx.doi.org/10.2471/blt.11.088302>
- Hartel, C. E. J., & Latemore, G. (2011). Mud and tears: The human face of disaster—A case study of the Queensland floods. *Journal of Management and Organization*, 17, 864-872. <http://dx.doi.org/10.5172/jmo.2011.864>
- Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996).
- Heller, N. A. (2012). Leadership in crisis: An exploration of the British Petroleum case. *International Journal of Business and Social Science*, 3(18) Retrieved from [http://ijbssnet.com/journals/Vol\\_3\\_No\\_18\\_Special\\_Issue\\_September\\_2012/4.pdf](http://ijbssnet.com/journals/Vol_3_No_18_Special_Issue_September_2012/4.pdf)
- Hemond, Y., & Benoit, R. (2012). Preparedness: the state of the art and future prospects. *Disaster Prevention and Management*, 21, 404-417. <http://dx.doi.org/10.1108/09653561211256170>
- Henstra, D. (2010). Evaluating local government emergency management programs: What framework should public managers adopt? *Public Administration Review*, 70, 236-246. <http://dx.doi.org/10.1111/j.1540-6210.2010.02130.x>
- Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, 52, 978-1002. <http://dx.doi.org/10.1080/00076791.2010.511185>
- Hickman, K. E. (2012). Navigating a transition in U.S. tax administration. *EJournal of Tax Research*, 10(2), 329-344. Retrieved from <http://search.proquest.com.proxy1.ncu.edu/docview/1115475928?accountid=28180>
- Hicks, L. (2011). *Informed consent*. Retrieved from <https://www.citiprogram.org/>
- Holt, T. P. (2012). The effects of internal audit role and reporting relationships on investor perceptions of disclosure credibility. *Managerial Auditing Journal*, 27, 878-898. <http://dx.doi.org/10.1108/02686901211263085>

- Hoong, L. L., & Marthandan, G. (2014). Critical dimensions of disaster recovery planning. *International Journal of Business and Management*, 9(12), 145-158. <http://dx.doi.org/10.5539/ijbm.v9n12p145>
- Houston, J. B., Pfefferbaum, B., & Rosenholtz, C. E. (2012). Disaster news: Framing and frame changing in coverage of major U.S. natural disasters, 2000-2010. *Journalism and Mass Communication Quarterly*, 89, 606-623. <http://dx.doi.org/10.1177/1077699012456022>
- Hosban, A., & Hamdan, M. N. (2015). Role for internal auditor to cope with IT risks and IT infrastructure in Jordan commercial banks. *International Journal of Business and Management*, 10, 295-304. <http://dx.doi.org/10.5539/ijbm.v10n3p295>
- Information Systems Audit and Control Association (ISACA). (2012). *Business continuity management: Emerging trends*. Retrieved from [http://www.infosecurityeurope.com/\\_novadocuments/48836?v=635307737294830000](http://www.infosecurityeurope.com/_novadocuments/48836?v=635307737294830000)
- Izumi, T., & Shaw, R. (2015). Disaster risk reduction, method, approaches, and practices. *Disaster Management and Private Sectors: Challenges and Potentials*. [http://dx.doi.org/10.1007/978-4-431-55414-1\\_1](http://dx.doi.org/10.1007/978-4-431-55414-1_1)
- Jahangiri, K., Izadkhah, Y. O., & Seyed, J. T. (2011). Disaster prevention and management. *Public Health and Safety*, 20, 82-94. <http://dx.doi.org/10.1108/09653561111111108>
- Jalba, L. G. (2013). Management and internal audit in the current context. *Knowledge Horizons.Economics*, 5, 118-121. Retrieved from [http://www.orienturi.ucdc.ro/arhiva/2013\\_KHE\\_PDF\\_Vol\\_5\\_SI\\_1/KHE\\_Vol\\_5\\_SIss\\_1\\_118to121.pdf](http://www.orienturi.ucdc.ro/arhiva/2013_KHE_PDF_Vol_5_SI_1/KHE_Vol_5_SIss_1_118to121.pdf)
- Jan, A., & Lurie, N. (2012). Disaster resilience and people with functional needs. *The New England Journal of Medicine*, 367, 2272-2273. <http://dx.doi.org/10.1056/nejmp1213492>
- Jarvelainen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, 20, 332-349. <http://dx.doi.org/10.1108/09685221211286511>
- Jensen, J. (2011). The current NIMS implementation behavior of the United States counties. *Journal of Homeland Security and Emergency Management*, 8(1), 1-25. <http://dx.doi.org/10.2202/1547-7355.1815>
- Jeya, J. J., & Kannan, E. (2014). Efficient ranked and secure file retrieval in cloud computing. *American Journal of Applied Sciences*, 11, 906-911. <http://dx.doi.org/10.3844/ajassp.2014.906.911>

- Johnsen, S. O., & Veen, M. (2013). Risk assessment and resilience of critical communication infrastructure in railways. *Cognition, Technology & Work*, 15, 95-107. <http://dx.doi.org/10.1007/s10111-011-0187-2>
- Johnson, P. (2010, June 1). Government's growing role could be an opportunity for comms strategists. *PRweek*. Retrieved from <http://www.prweek.com/article/governments-growing-role-opportunity-comms-strategists/1267552>
- Johnston, D., Becker, J., & Paton, D. (2012). Multi-agency community engagement during disaster recovery. *Disaster Prevention and Management*, 21, 252-268. <http://dx.doi.org/10.1108/09653561211220034>
- Jones, V.A. (2011). How to avoid disaster: RIM's crucial role in business continuity planning. *Information Management*, 45(6). 36-40. Retrieved from <http://content.arma.org/IMM/November-December2011/rimfundamentalshowtoavoiddisaster.aspx>.
- Kamel, H., & Elkhatib, S. (2013). The perceptions of audit committees' role in an emerging market: The case of Egypt. *Journal of Economic and Administrative Sciences*, 29, 85-98. <http://dx.doi.org/10.1108/jeas-09-2013-0028>
- Kanellou, A., & Spathis, C. (2011). Auditing in enterprise system environment: A synthesis. *Journal of Enterprise Information Management*, 24, 494-519. <http://dx.doi.org/10.1108/17410391111166549>
- Kantur, D., & Arzu, I. (2012). Organizational resilience: A conceptual integrative framework. *Journal of Management and Organization*, 18, 762-773. <http://dx.doi.org/10.5172/jmo.2012.18.6.762>
- Karim, A.J. (2011). Business disaster preparedness: An empirical study for measuring the factors of business continuity to face business disaster. *International Journal of Business and Social Science*, 2(18). Retrieved from [http://ijbssnet.com/journals/Vol\\_2\\_No\\_18\\_October\\_2011/23.pdf](http://ijbssnet.com/journals/Vol_2_No_18_October_2011/23.pdf)
- Kent, P. (2011). The decision to outsource management advisory services. *Managerial Auditing Journal*, 26, 672-696. <http://dx.doi.org/10.1108/02686901111161331>
- Klein, H. K. (2012). Principles for insurance regulation: An evaluation of current practices and potential reforms. *Geneva Papers on Risk & Insurance*, 37(1), 175-199. <http://dx.doi.org/10.1057/gpp.2011.9>
- Koronis, E., & Ponis, S. T. (2012). Introducing corporate reputation continuity to support organizational resilience against crises. *Journal of Applied Business Research*, 28, 283-290. <http://dx.doi.org/10.19030/jabr.v28i2.6850>
- Kotb, A., Sangster, A., & Henderson, D. (2014). E-business internal audit: The elephant is still in the room! *Journal of Applied Accounting Research*, 15, 43-63. <http://dx.doi.org/10.1108/jaar-10-2012-0072>

- Krishnan, G. V., & Yu, W. (2012). Do small firms benefit from auditor attestation of internal control effectiveness. *Auditing: A Journal of Practice and Theory*, 31(4), 115-137. <http://dx.doi.org/10.2308/ajpt-50238>
- Kruger, S. (2009). Local emergency management funding: An evaluation of county budgets. *Journal of Homeland Security and Emergency Management*, 6(1), Article 43. <http://dx.doi.org/10.2202/1547-7355.1434>
- Kunreuther, H., & Michel-Kerjan, E. (2011). People get ready disaster preparedness. *Issues in Science and Technology*, 28(1), 39-50. Retrieved from [http://opim.wharton.upenn.edu/risk/library/J2011IST\\_PeopleGetReady.pdf](http://opim.wharton.upenn.edu/risk/library/J2011IST_PeopleGetReady.pdf).
- Kusumasari, B., Alam, Q., & Siddiqui, K. (2010). Resource capability for local government in managing disaster. *Disaster Prevention and Management*, 19, 438-451. <http://dx.doi.org/10.1108/09653561011070367>
- Lasecki, A. J. (2009). *Assessing and exploring strategic business continuity planning methods in Michigan small businesses* (Doctoral dissertation). Retrieved from the ProQuest Theses and Dissertations database. (UMI No. 3368182)
- Law, M. D., & Robson, G. (2014). A case study for accounting information systems - A business continuity plan for protecting critical financial information in the NYC financial services industry. *The Review of Business Information Systems*, 18(1), 15-22. <http://dx.doi.org/10.19030/rbis.v18i1.8539>
- Lee, A. C. K., Booth, A., Challen, K., Gardois, P., & Goodacre, S. (2014). Disaster management in low- and middle-income countries: Scoping review of the evidence base. *Emergency Medicine Journal: EMJ*, 31. <http://dx.doi.org/10.1136/emmermed-2013-203298>
- Lee, K., Lan, L., Wang, J., Fang, C., & Shiao, K. (2014). How to reduce the latent social risk of disease: The determinants of vaccination against rabies in Taiwan. *International Journal of Environmental Research and Public Health*, 11, 5934-5950. <http://dx.doi.org/10.3390/ijerph110605934>
- Lehman, C.M. (2010). Issues in accounting education. *American Accounting Association*, 25(4), 741-754. <http://dx.doi.org/10.2308/iace.2010.25.4.741>
- Lenz, R., & Sarens, G. (2012). Reflections on the internal auditing profession: What might have gone wrong? *Managerial Auditing Journal*, 27, 532-549. <http://dx.doi.org/10.1108/02686901211236382>
- Lester, S. A. G., & Persia, A. M. (2011). Disaster risk reduction for health facilities in the Western Pacific Region. *International Journal of Disaster Resilience in the Built Environment*, 2, 268-277. <http://dx.doi.org/10.1108/17595901111167132>

- Leung, P., Cooper, B. J., & Perera, L. (2011). Accountability structures and management relationships of internal audit. *Managerial Auditing Journal*, 26, 794-816. <http://dx.doi.org/10.1108/02686901111171457>
- Leverly, J.T. (2012). The cost of duplicative regulation: Evidence from risk retention groups. *Journal of Risk and Insurance*, 79, 105-127. <http://dx.doi.org/10.1111/j.1539-6975.2011.01437.x>
- Lindell, M. K., Prater, C., & Perry, R. W. (2007). *Introduction to emergency management*. Hoboken, NJ: Wiley and Sons.
- Lindberg, D. L., & Seifert, D. L. (2011). Enterprise risk management (ERM) can assist insurance in complying with the Dodd-Frank Act. *Journal of Insurance Regulation*, 30, 319-337. Retrieved from [http://www.naic.org/prod\\_serv\\_jir.htm](http://www.naic.org/prod_serv_jir.htm)
- Lindström, J. (2012). A model to explain a business contingency process. *Disaster Prevention and Management*, 12, 269-281. <http://dx.doi.org/10.1108/09653561211220052>
- Lindström, J., Samuelson, S., & Hägerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management*, 19, 243-255. <http://dx.doi.org/10.1108/09653561011038039>
- Luftman, J., & Zadeh, H. S. (2011). Key information technology and management issues. *Journal of Information Technology*, 26, 193-204. <http://dx.doi.org/10.1057/jit.2011.3>
- Malalgoda, C., Amaratunga, D., & Haigh, R. (2013). Creating a disaster resilient built environment in urban cities. *International Journal of Disaster Resilience in the Built Environment*, 4, 72-94. <http://dx.doi.10.1108/17595901311299017>
- Marques, M. d. C. d. C. (2014). Internal audit in the public sector as a tool for risk prevention of corruption in public administration in Portugal. *Business and Management Research*, 3(3), 1-10. <http://dx.doi.org/10.5430/bmr.v3n3p43>
- Marsh, T., Fischer, M., & Montondon, L.(2013). Government's new normal: A changing role for auditors. *The Journal of Government Financial Management*, 62(3), 12-17. Retrieved from <http://www.howtomanuals.net/how-are-governments-coping-with-the-new-normal-tgd.html?page=6>
- Matuk, J., & Young, B. (2011). *Records-based research*. Retrieved from <https://www.citiprogram.org/>
- Maurice, J. (2013). Mitigating disasters—a promising start. *The Lancet*, 381, 1611-1613. [http://dx.doi.org/10.1016/S0140-6736\(13\)61008-9](http://dx.doi.org/10.1016/S0140-6736(13)61008-9)

- McEntire, D. (2012). Understanding and reducing vulnerability: from the approach of liabilities and capabilities. *Disaster Prevention and Management*, 21(2), 206-255. <http://dx.doi.org/10.1108/09653561211220007>
- McGrady, E., & Blanke, S. J. (2014). Twelve best practices to mitigate risk through continuity planning and a scorecard to track success. *Journal of Management Policy and Practice*, 15(3), 11-19. Retrieved from [http://www.na-businesspress.com/JMPP/McGradyE\\_Web15\\_3\\_.pdf](http://www.na-businesspress.com/JMPP/McGradyE_Web15_3_.pdf)
- McGuire, M., & Schneck, D. (2010). What if hurricane Katrina hit in 2020? The need for strategic management of disasters. *Public Administration Review*, 70, S201-S207. <http://dx.doi.org/10.1111/j.1540-6210.2010.02273.x>
- Medders, L., McCullough, K., & Jäger, V. (2011). Tale of two regions: Natural catastrophe insurance and regulation in the United States and the European Union. *Journal of Insurance Regulation*, 30(1), 171-196
- Mekdeci, K. B. (2011). *Educational technology: Transitioning from business continuity to mission continuity* (Doctoral dissertation, Lehigh University). Retrieved from <http://preserve.lehigh.edu/cgi/viewcontent.cgi?article=2179&context=etd>
- Melnik, T. (2015). New U.S. sanctions program seeks to give government an extra tool to fight cyber-attacks. *Journal of Health Care Compliance*, 17(3), 53-56. Retrieved from [http://melniklegal.com/av/2015\\_05\\_JHCC\\_US\\_Sanctions.pdf](http://melniklegal.com/av/2015_05_JHCC_US_Sanctions.pdf)
- Mix, V. (2012). Renovation and roadblocks while protecting the collection. *Collection Building*, 31, 153-157. <http://dx.doi.org/10.1108/01604951211274061>
- Moeller, R. R. (2008). *Sarbanes-Oxley and the new internal auditing rules* (1st ed.). Hoboken, NJ: Wiley
- Momani, N.M. (2010). Business continuity planning: Are we prepared for future disasters? *American Journal of Economic and Business Administration*, 2(3), 272-279. Retrieved from <http://thescipub.com/pdf/10.3844/ajebasp.2010.272.279>
- Mukhtar, S. A. (2013). Organizational conflict management strategies on employee job satisfaction: A conceptual relationship. *International Journal of Management Research and Reviews*, 3, 2855-2862. Retrieved from [http://ijmrr.com/admin/upload\\_data/journal\\_SA%20Mukhtar%20%203may13mrr.pdf](http://ijmrr.com/admin/upload_data/journal_SA%20Mukhtar%20%203may13mrr.pdf)
- Munro, D. (2011). *The allocation of federal homeland Security grant funds in Riverside county California* (Doctoral dissertation). Retrieved from the Proquest Theses and Dissertations database. (UMI No. 3443903)
- Muqattash, R. (2011). The effect of the factors in the internal audit department on the internal auditors objectivity in the bank operating in the United Arab Emirates. *Journal of International Management Studies*, 6(3), 92-100. Retrieved from <http://www.iabe.org/domains/iabeX/journalinfo.aspx?JournalID=JIMS>



- Nasim, S., & Sushil. (2010). Managing continuity and change: A new approach for strategizing in e-government. *Transforming Government: People, Process and Policy*, 4(4), 338-364. <http://dx.doi.org/10.1108/17506161011081327>
- Năstase, P., & Unchiașu, S. F. (2013). Implications of the operational risk practices applied in the banking sector on the information systems area. *Accounting and Management Information Systems*, 12(1), 101-117. Retrieved from [http://www.cig.ase.ro/articles/12\\_1\\_6.pdf](http://www.cig.ase.ro/articles/12_1_6.pdf)
- Nicoll, S. R., & Owens, R. W. (2013). Emergency response and business continuity. *Professional Safety*, 50-55. Retrieved from [http://www.asse.org/professionalsafety/pastissues/058/09/F1Nic\\_0913.pdf](http://www.asse.org/professionalsafety/pastissues/058/09/F1Nic_0913.pdf).
- Niemimaa, M., & Jarvelainen, J. (2013). IT service continuity: Achieving embeddedness through planning. In *availability, reliability, and security (ARES), 2013 Eighth International Conference*, 333-340. <http://dx.doi.org/10.1109/ares.2013.45>
- Nor Azimah, A. A. (2013). Managing corporate risk and achieving internal control through statutory compliance. *Journal of Financial Crime*, 20(1), 25-38. <http://dx.doi.org/10.1108/13590791311287328>
- Novriansa, A., & Riyanto, B. (2016). Role conflict and role ambiguity on local government internal auditors: the determinant and impacts. *Journal of Indonesian Economy and Business*, 31, 63-82. Retrieved from <http://jurnal.ugm.ac.id/jieb>
- NYSE Corporate Governance Listing Standards (2013). *Section 303A of the NYSE's Listed*. Retrieved from [https://www.nyse.com/pdfs/section303A\\_final\\_rules](https://www.nyse.com/pdfs/section303A_final_rules).
- Odoyo, F. S., Omwono, G. A., & Okinyi, N. O. (2014). An analysis of the role of internal audit in implementing risk management: A study of state corporations in Kenya. *International Journal of Business and Social Science*, 5(6), 169-176. Retrieved from [http://www.ijbssnet.com/journals/vol\\_5\\_no\\_6\\_may\\_2014/18.pdf](http://www.ijbssnet.com/journals/vol_5_no_6_may_2014/18.pdf).
- Office of Management & Budget (2011). *Federal Register* 76(123), 56227-56242. Retrieved from <http://www.gpo.gov/fdsys/pkg/FR-2011-09-12/pdf/2011-23165.pdf>
- Oh, N. (2012). Strategic uses of lessons for building collaborative emergency management system: Comparative analysis of Hurricane Katrina and Hurricane Gustav response systems. *Journal of Homeland Security and Emergency Management*, 9(1), 1-20. <http://dx.doi.org/10.1515/1547-7355.1765>
- Ojha, D., Gianiodis, P. T., & Manuj, I. (2013). Impact of logistical business continuity planning on operational capabilities and financial performance. *International Journal of Logistics Management*, 24, 180-209. <http://dx.doi.org/10.1108/ijlm-06-2012-0049>

- Ojha, D., & Gokhale, R.A. (2009). Logistical business continuity planning-scale development and validation. *International Journal of Logistics Management*, 20, 342-359. <http://dx.doi.org/10.1108/09574090911002814>
- Omar, A., Alijani, D., & Mason, R. (2011). Information technology disaster recovery plan: case study. *Academy of Strategic Management Journal*, 10, 127-141. Retrieved from <http://suno.edu/Chancellor/docs/SUNO2010-2011AnnualReport.pdf>.
- Ostrander, I., & Lowry, W. R. (2012). Oil crises and policy continuity: A history of failure to change. *Journal of Policy History*, 24, 384-404. <http://dx.doi.org/10.1017/S0898030612000115>
- Palliyaguru, R., Amaratunga, D., & Haigh, S. (2010). Integration of “disaster risk reduction” into infrastructure reconstruction sector: Policy vs practice gaps. *International Journal of Disaster Resilience in the Built Environments*, 1, 277-296. <http://dx.doi.org/10.1108/17595901011080878>
- Pang, Y., & Li, Q. (2013). Game analysis internal control and risk management. *International Journal of Business and Management*, 8(17), 103-111. <http://dx.doi.org/10.5539/ijbm.v8n17p103>
- Parker, R. (2011). All-hazards resilience: A paradigm for the 21st century. *Defence S&T Technical Bulletin*, 4(1), 56-63. Retrieved from <http://www.myjournal.my>
- Pathirage, C., Seneviratne, K., Amaratunga, D., & Haigh, R. (2012). Managing disaster knowledge: Identification of knowledge factors and challenges. *International Journal of Disaster Resilience in the Built Environment*, 3, 237-252. <http://dx.doi.org/10.1108/17595901211263620>
- Patterson, O., Weil, F., & Patel, K. (2010). The role of community in disaster response: Conceptual models. *Population Research and Policy Review*, 29, 127-141. <http://dx.doi.org/10.1007/s11113-009-9133-x>
- Patton, M. Q. (2002). *Qualitative research & evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage.
- Paul, D. (2012). *Informed consent*. Retrieved from <https://www.citiprogram.org/>
- Pearson, D. D. R. (2010). Business continuity management in local government (Victorian Auditor-General’s report, PP No. 355, Session 2006-10). Retrieved from <http://www.audit.vic.gov.au/publications/2010-11/20100109-bus-cont-full-report.pdf>
- Pelfrey, W. V., Sr., & Kelley, W. D., Jr. (2013). Homeland security education: A way forward. *Homeland Security Affairs*, 9, Art. 3. Retrieved from <https://www.hsaj.org/articles/235>

- Pheng, L. S., Ying, L. J., & Kumaraswamy, M. (2010). Institutional compliance framework and business continuity management in mainland China, Hong Kong SAR and Singapore. *Disaster Prevention and Management*, 19, 596-614. <http://dx.doi.org/10.1108/09653561011091922>
- Pierson, M. (2013). Characteristics of a knowledge harvesting and management system. *TechTrends*, 57(2), 26-32. <http://dx.doi.org/10.1007/s11528-013-0642-4>
- Pinta, J. (2011). Disaster recovery planning as part of business continuity management. *AGRIS on-Line Papers in Economics and Informatics*, 3(4), 55-61. Retrieved from <http://purl.umn.edu/120243>
- Raman, M., Dorasamy, M., Muthaiyah, S., Kaliannan, M., & Muthuveloo, R. (2011). Knowledge management for social workers involved in disaster planning and response in Malaysia: An action research approach. *Systemic Practice and Action Research*, 24, 261-272. <http://dx.doi.org/10.1007/s11213-011-9193-9>
- Ramiah, V., & Graham, M. (2013). The impact of domestic and international terrorism on equity markets: Evidence from Indonesia. *International Journal of Accounting and Information Management*, 21, 91-107. <http://dx.doi.org/10.1108/18347641311299768>
- Randeree, K., Mahal, A., & Narwani, A. (2012). A business continuity management maturity model for the UAE banking sector. *Business Process Management Journal*, 18, 472-492. <http://dx.doi.org/10.1108/14637151211232650>
- Reid, E., Waring, M., Enriquez, C. R., & Shivdas, M. (2012). Embracing disruptions, responding to uncertainties, valuing agency: Situating a feminist approach to social protection. *Development*, 55, 291-298. <http://dx.doi.org/10.1057/dev.2012.30>
- Renaud, C. (2012). The missing piece of NIMS: Teaching incident commanders how to function in the edge of chaos. *Homeland Security Affairs*, 8(8), 1-19. Retrieved from <https://www.hsaj.org/articles/221>
- Resnick, M. D. (1987). *Choices: An introduction to decision theory*. Minneapolis, MN: University of Minnesota Press.
- Rodriguez, H., Quarantelli, E. L., & Dynes, R. (Eds.). (2007). *Handbook of disaster research*. New York, NY: Springer.
- Rosenberg, N. A. (2014). 10 Steps to implement a disaster recovery plan. Retrieved from Quality Technology Solutions website: <http://www.qtsnet.com/>
- Santos, R. S., Borges, M. R. S., Canós, J. H., & Gomes, J. O. (2011). The assessment of information technology maturity in emergency response organizations. *Group Decision and Negotiation*, 20, 593-613. <http://dx.doi.org/10.1007/s10726-011-9232-z>

- Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745 (2002).
- Sarens, G., Abdolmohammadi, M. J., & Lenz, R. (2012). Factors associated with the internal audit function's role in corporate governance. *Journal of Applied Accounting Research*, 13, 191-204. <http://dx.doi.org/10.1108/09675421211254876>
- Sawalha, I. H. S., Anchor, J. R., & Meaton, J. (2012). Business continuity management in Jordanian banks: Some cultural considerations. *Risk Management*, 14, 301-324. <http://dx.doi.org/10.1057/rm.2012.10>
- Sawalha, I. H. S., Jraisat, L. E., & Al-Qudah, K. A. M. (2013). Crisis and disaster management in Jordanian hotels: Practices and cultural considerations. *Disaster Prevention and Management*, 22, 210-228. <http://dx.doi.org/10.1108/dpm-09-2012-0101>
- Schram, T. H. (2006). *Conceptualizing and proposing qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson.
- Seago, J., (2015). A new framework for a new age. *Internal Auditor: Journal of the Institute of Internal Auditors*, 1-6. Retrieved from <https://iaonline.theiia.org/2015/a-new-framework-for-a-new-age>
- Shank, G. D. (2006). *Qualitative research a personal skills approach*, Upper Saddle River, NJ: Pearson Merrill Prentice Hall.
- Schneider, G. P., Sheikh, A., & Simione, K. A. (2012). Holistic risk management: An expanded role for internal auditors. *Academy of Accounting and Financial Studies Journal*, 16(1), 25-33. Retrieved from [www.alliedacademies.org/public/journals/JournalDetails.aspx?jid=21](http://www.alliedacademies.org/public/journals/JournalDetails.aspx?jid=21)
- Scott, W. D., & Nganje, W. (2011). An ex-post evaluation of Sarbanes-Oxley Acton firm's intrinsic value: A principal-agent framework. *Academy of Accounting and Financial Studies Journal*, 15(3), 95-118. Retrieved from <http://www.freepatentsonline.com/article/Academy-Accounting-Financial-Studies-Journal/263035501.html>
- Shughart, W. F. (2011). Disaster relief as bad public policy. *The Independent Review*, 15, 519-539. Retrieved from [http://www.independent.org/pdf/tir\\_15-04\\_2\\_shughart.pdf](http://www.independent.org/pdf/tir_15-04_2_shughart.pdf)
- Sinason, D. H. (2011). Internal audit lessons from the disaster in Japan. *Internal Auditing*, 26(3), 3-8. Retrieved from <http://search.proquest.com.proxy1.ncu.edu/docview/872082216?accountid=28180>
- Smit, N. (2005). *Business continuity management: A maturity model* (Master's thesis, Erasmus University Rotterdam). Retrieved from <http://docplayer.net/605903-Business-continuity-management-a-maturity-model-by-naomi-smit.html>

- Smith, J. (2013). Strategic continuity planning: The first critical health policy and management departments: Ensuring educational continuity step. *Journal of Business Continuity & Emergency Planning*, 7(1), 6-12. Retrieved from <http://www.henrystewartpublications.com/jbcep>.
- Soh, S. B. D., & Martinov-Bennie, N. (2011). The internal audit function. *Managerial Auditing Journal*, 26, 605-622. <http://dx.doi.org/10.1108/02686901111151332>
- Soltani, B. (2014). The anatomy of corporate fraud: A comparative analysis of high profile American and European corporate scandals. *Journal of Business Ethics*, 120, 251-274. <http://dx.doi.org/10.1007/s10551-013-1660-z>
- Sorial, S. (2011). Politics of violence. *Critical Horizons*, 12, 163-164. <http://dx.doi.org/10.1558/crit.v12i2.163>
- SORM (2016). *Continuity of operations*. Retrieved from [www.sorm.state.tx.us/coop](http://www.sorm.state.tx.us/coop)
- SORM (2016). *Texas state agency continuity planning policy guidance letter*. Retrieved from [www.sorm.state.tx.us/coop/texas-coop](http://www.sorm.state.tx.us/coop/texas-coop)
- Spremic, M., Jakovic, B., Braje, I. N., & Cavlek, N. (2013). The impact of the enterprise resource planning systems on company's E-business efficiency. *Journal of American Business Review, Cambridge*, 2(1), 276-282. Retrieved from <http://search.proquest.com.proxy1.ncu.edu/docview/1466276725?accountid=28180>
- Staley, J; Zelman, W., Porto, J., Hobbs, S., & Paul, J. (2009). Preparedness roles for health policy and management departments: Ensuring educational continuity during disaster events. *The Journal of Health Administration Education*, 26(4), 309-321. Retrieved from <http://www.aupha.org/publications/journalofhealthadministrationeducation>
- Stallings, R. A. (2007). Methodologies issues. Methodological issues. In H. Rodriguez, E. L. Quarantelli, & R. R. Dynes (Eds.), *Handbook of disaster research* (pp. 55-82). New York, NY: Springer.
- Stefaniak, C. M., Houston, R. W., & Cornell, R. M. (2012). The effects of employer and client identification on internal and external auditors' evaluations of internal control deficiencies. *Auditing*, 31, 39-56. <http://dx.doi.org/10.2308/ajpt-10179>
- Sterbenz, J. P. G., Çetinkaya, E. K., Hameed, M. A., Jabbar, A., Qian, S., & Rohrer, J. P. (2013). Evaluation of network resilience, survivability, and disruption tolerance: Analysis, topology generation, simulation, and experimentation. *Telecommunication Systems*, 52, 705-736. <http://dx.doi.org/10.1007/s11235-011-9573-6>

- Stewart, J., & Subramaniam, N. (2010). Internal audit independence and objectivity: emerging research opportunities. *Managerial Auditing Journal*, 23, 328-360. <http://dx.doi.org/10.1108/02686901011034162>
- Sudmeier, K. I., Jaboyedoff, M., & Jaquet, S. (2013). Operationalizing "resilience" for disaster risk reduction in mountainous Nepal. *Disaster Prevention and Management*, 22, 366-377. <http://dx.doi.org/10.1108/dpm-02-2013-0028>
- Sun, L. G. (2011). Smart growth in dumb places: Sustainability, disaster, and the future of the American City. *Brigham Young University Law Review*, 2011, 2157-2201. <http://dx.doi.org/10.2139/ssrn.1918386>
- Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative Research Journal*, 11(2), .63-75 <http://dx.doi.org/10.3316/qrJ1102063>
- Texas State Auditor's Office (2015). *Texas State Internal Audit Contacts*. Retrieved from <https://www.sao.state.tx.us/Resources/IntAud/contacts.aspx>
- Texas Internal Auditing Act. (2003). Retrieved from <http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.2102.htm>
- Texas Legislature, 80th Legislative Session, Regular Session. (2007). Retrieved from <http://www.statutes.legis.state.tx.us/Docs/LA/htm/LA412.htm>
- Texas State Office of Risk Management. (2016). *Continuity*. Retrieved from <https://www.sorm.state.tx.us/coop>
- Thach, L. (2012). Managerial perceptions of crisis leadership in public and private organizations: An interview study in the United States. *International Journal of Management*, 29, 712-725. Retrieved from <http://www.theijm.com/>
- Tudoran, L. E., & Ionescu, B. S. (2014). The use of accounting APPS via mobile cloud computing in Romania. *Annales Universitatis Apulensis : Series Oeconomica*, 16, 294-303. <http://dx.doi.org/10.13140/2.1.5050.2087>
- Turulj, L., & Bajgoric, N. (2012). Being prepared for disaster? Implementation of business continuity planning concept in B&H organizations. *Conference Proceedings: International Conference of the Faculty of Economics Sarajevo (ICES)*, 448-459. <http://dx.doi.org/10.1007/s11235-011-9573-6>
- Tysiac, J. (2012). Internal Control, revisited. *Journal of Accountancy*, 213(3), 24-29. Retrieved from <http://www.journalofaccountancy.com/issues/2012/mar/20114943.html>

- Verchick, R. R. M., & Hall, A. (2011). Adapting to climate change while planning for disaster: Footholds, rope lines, and the Iowa floods. *Brigham Young University Law Review*, 2011, 2203-2260. Retrieved from <http://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=2631&context=lawreview>
- Vissak, T. (2010). Recommendations for using the case study method in international business research. *The Qualitative Report*, 15, 370-388. Retrieved from <http://www.nova.edu/ssss/QR/QR15-2/vissak.pdf>
- Warren, C. M. J (2010). The role of public sector asset managers in responding to climate change: Disaster and business continuity planning. *Property Management*, 28, 245-256. <http://dx.doi.org/10.1108/02637471011065674>
- Wayman, M. (2013). Curbing outsourcing risks: Internal audit should examine closely the oversight of the organization's third-party relationships to enhance effective governance and decrease risk. *Internal Auditor: Journal of the Institute of Internal Auditors*, 70, 41-44. <http://dx.doi.org/10.1007/s11235-011-9573-6>
- Weber, J., & Wasieleski (2013). Corporate ethics and compliance programs: A report, analysis and critique. *Journal of Business Ethics*, 112, 609-626. <http://dx.doi.org/10.1007/s10551-012-1561-6>
- Wedawatta, G., & Ingirige, B. (2012). Resilience and adaptation of small and medium-sized enterprises to flood risk. *Disaster Prevention and Management*, 21, 474-488. <http://dx.doi.org/10.1108/09653561211256170>
- Wees, A. (2013). *Requirements for business contingency and continuity plans* (CSEC650, 9045). Retrieved from RESEARCHEDSOLUTION website: <https://researchedsolution.wordpress.com/2013/09/14/requirements-for-business-contingency-and-continuity-plans/>
- Wines, G. (2012). Auditor independence. *Managerial Auditing Journal*, 27(1), 5-40. <http://dx.doi.org/10.1108/02686901211186081>
- Yin, R. K. (2009). *Case study research design and methods* (4th ed.). Thousand Oaks, CA: Sage.
- Yoon, D. K., Youngs, G. A. Jr., & Abe, D. (2012), Examining factors contributing to the development of FEMA-approved hazard mitigation plans, *Journal of Homeland Security and Emergency Management*, 9(2), 1-18. doi:10.1515/1547-7355.2010
- Zaharia, D. L., Dragne, L., & Tilea, D. M. (2014). The modern practice of internal auditing in the context of globalization. *Knowledge Horizons Economics*, 6, 174-176. Retrieved from [http://www.orizonturi.ucdc.ro/arhiva/2014\\_khe\\_62\\_p ... 6\\_iss\\_2\\_174to176.pdf](http://www.orizonturi.ucdc.ro/arhiva/2014_khe_62_p...6_iss_2_174to176.pdf)

- Zain, M. M., Zaman, M., & Mohamed, Z. (2015). The effect of internal audit function quality and internal audit contribution to external audit on audit fees. *International Journal of Auditing*, 19, 134-147. <http://dx.doi.org/10.1111/ijau.12043>
- Zaman, M., & Sarens, G. (2013). Informal interactions between audit committees and internal audit functions. *Managerial Auditing Journal*, 28(6), 495-515. <http://dx.doi.org/10.1108/02686901311329892>
- Zerni, M. (2012). Do client firms manage the perception of auditor independence? *Managerial Auditing Journal*, 27, 821-845. <http://dx.doi.org/10.1108/02686901211263067>



Appendices

### Appendix A: Recruitment Letter - Telephone Script

My name is Monday N. Rufus, and I am a Ph.D. candidate at Northcentral University in Prescott, Arizona. I am under the supervision of Dr. Edward Kim, Dissertation Chair. I am recruiting government sector internal auditors to participate in my dissertation research study. The study explores business continuity planning and the role internal auditors play in the government sector. The results of this case study are intended to benefit internal auditors and government sector in helping protect the interests of the public. To participate, you must currently be an internal auditor working in the State of Texas. You must also be between 18 and 65 years of age.

Participation will consist of a one-on-one interview in person or on the phone, and will last between 30–45 minutes. Participation is completely voluntary, and you may stop the interview at any time. To ensure your protection, names and identities will not be disclosed to anyone at any time. Prior to the interview, you will be asked to sign an Informed Consent Form. This form will provide a complete overview of what will be asked of you. This overview includes how your privacy will be protected, and the uses of the interview data.

Thank you in advance for your time. If you have any questions, please feel free to contact me at [M.Rufus9407@email.ncu.edu](mailto:M.Rufus9407@email.ncu.edu) or via phone at 512-775-3698.

This study has received approval from the Northcentral University Institutional Review Board (IRB #2016).

## Appendix B: Recruitment Letter - Email Script

As discussed over the phone, my name is Monday N. Rufus, and I am a Ph.D. candidate at Northcentral University in Prescott, Arizona. I am under the supervision of Dr. Edward Kim, Dissertation Chair.

I am recruiting government sector internal auditors to participate in my dissertation research study. The study explores business continuity planning and the role internal auditors play in the government sector. The results of this case study are intended to benefit internal auditors and government sector in helping protect the interests of the public. To participate, you must currently be an internal auditor working in the State of Texas. You must also be between 18 and 65 years of age.

Participation will consist of a one-on-one interview in person or on the phone, and will last between 30–45 minutes. Participation is completely voluntary, and you may stop the interview at any time. To ensure your protection, names and identities will not be disclosed to anyone at any time. Prior to the interview, you will be asked to sign an Informed Consent Form. This form will provide a complete overview of what will be asked of you. This overview includes how your privacy will be protected, and the uses of the interview data.

Thank you in advance for your time. If you have any questions, please feel free to contact me at [M.Rufus9407@email.ncu.edu](mailto:M.Rufus9407@email.ncu.edu) or via phone at 512-775-3698.

This study has received approval from the Northcentral University Institutional Review Board (IRB #2016).

## Appendix C: IRB Approval



**Date:** 2/1/2016  
**PI Name:** Monday Rufus  
**Chair Name (if applicable):** Dr. Edward Kim  
**Application Type (Initial, Modification, Continuing, Pilot):** Initial  
**Review Level (Exempt, Expedited, Full Board):** Expedited, Cat 7  
**Study Title:** Perceived Roles of the Internal Auditor in Business Continuity Planning in the Government Sector

<p><b>Approval Date:</b> 2/1/2016  <b>Continuing Review Due Date:</b> 2/1/2017  <b>Expiration Date:</b> 2/1/2017</p>
--

Dear Monday:

Congratulations! The purpose of this letter is to inform you that your IRB application has been approved. Your responsibilities include the following:

1. Follow the protocol as approved. If you need to make changes, please submit a modification form requesting approval of any proposed changes before you make them.
2. If there is a consent process in your research, you must use the consent form approved with your final application. Please make sure all participants receive a copy of the consent form.
3. Continuing review is required as long as you are in data collection or if data have not been de-identified. Failure to receive approval of the continuing review before the expiration date means the research must stop immediately.
4. If there are any injuries, problems, or complaints from participants, you must notify the IRB at [IRB@ncu.edu](mailto:IRB@ncu.edu) within 24 hours.
5. IRB audit of procedures may occur. The IRB will notify you if your study will be audited.
6. When data are collected and de-identified, please submit a study closure form to the IRB.
7. You must maintain current CITI certification until you have submitted a study closure form.
8. If you are a student, please be aware that you must be enrolled in an active dissertation course with NCU in order to collect data.

Congratulations from the NCU IRB. Best wishes as you conduct your research!

Respectfully,

Northcentral University Institutional Review Board  
 Email: [irb@ncu.edu](mailto:irb@ncu.edu)

2488 Historic Decatur Rd., Suite 100, San Diego, CA 92106 USA  
[www.ncu.edu](http://www.ncu.edu) · p: 928-541-8014 · f: 928-515-5519

## Appendix D: Informed Consent Form

**Introduction:**

My name is Monday N. Rufus. I am a doctoral student at Northcentral University. I am conducting a research study on the perceived roles of the internal auditor in business continuity planning in the government sector. I am completing this research as part of my doctoral degree. I invite you to participate.

**Activities:**

If you participate in this research, you will be asked to partake in a 30 to 45-minute interview over the phone or in person.

**Eligibility:**

You are eligible to participate in this research if you are identified as an internal auditor currently working in the State of Texas in the United States, and are between 18 and 65 years of age.

You are not eligible to participate in this research if:

1. You are less than 18 years or more than 65 years old
2. You are not working in the government sector as an internal auditor in the State of Texas.

I hope to include a sample 20 people in this research.

**Risks:**

There are minimal risks in this study. Some of the questions might be personally sensitive since they are asking your opinion on the perceived roles of the internal auditor in business continuity planning in the government sector. Additionally, some of the interviews may occur in a public setting like a coffee shop or restaurant where confidentiality will not be guaranteed. This can be uncomfortable for some people. Alternatively, the interview may occur at a public library where private rooms exist. You can choose to skip any questions that you feel uncomfortable in answering. You may also stop participating in the interview at any time.

**Benefits:**

If you decide to participate, there are no direct benefits to you.

**The potential benefits to others are:** The results of this case study could be useful to the government sector and their internal auditors as they continue to protect the interest of the public.

**Confidentiality:**

The information you provide will be kept confidential to the extent allowable by law. Some steps I will take to keep your identity confidential are not to link your name and your personal information to data collected. The researcher will be the only person who will see the data.

The people who will have access to your information are my dissertation committee and me. The Institutional Review Board may also review my research and view your information.

I will secure your information with these steps: securing it in a fireproof safe with a key combination only known to me. All electronic forms of data will be encrypted on my computer and password protected and computer transported in a locked case.

I will keep your data for 7 years. Then, I will delete electronic data and destroy paper data.

**Contact Information:**

If you have questions for me, you can contact me at M.Rufus9407@email.ncu.edu  
My dissertation chair's name is Dr. Edward Kim. He works at Northcentral  
University and is supervising me on the research. You can contact him at  
ekim@ncu.edu or on his office phone at 303-282-7448.

If you have questions about your rights in the research, or if a problem has occurred,  
or if you are injured during your participation, please contact the Institutional Review  
Board at irb@ncu.edu or 1-888-327-2877 ext 8014.

**Voluntary Participation:**

Your participation is voluntary. If you decide not to participate, or if you stop  
participation after you start, there will be no penalty to you. You will not lose any  
benefit to which you are otherwise entitled.

**Audiotaping:**

I would like to use a voice recorder to record your responses. You can still  
participate if you do not wish to be recorded. If so, I will ask you to verify my notes  
after the interview in person or via a telephone.

Please sign here if I can record you:

**Signature:**

A signature indicates your understanding of this consent form. You will be given a  
copy of the form for your information.

Participant Signature Printed Name Date

Researcher Signature Printed Name Date

## Appendix E: Interview Guide

I will follow the protocol below:

1. Identify potential participants.
2. Select individuals to be interviewed.
3. Email a Recruiting Letter to the individuals to be interviewed.

Explain the purpose of the study.

4. Set interviews with the participants and explain the purpose of the interview, why each individual was selected. Also, explain how long the interview will last.
5. Seek informed consent of the interviewee prior to beginning the interview.  
Reiterate the purpose of the study and interview, why the interviewee was selected, how long the interview will last, confidentiality, and tape recording.
6. After obtaining consent, I will conduct the interview using the questionnaire instrument developed. Interview questions will be open-ended
7. After the interview, I will obtain verification of notes, if the interviewee elected not to be tape recorded.

## Appendix F: Interview Questions

1. What are the perceived reasons why an organization such as a government agency should prepare for a disruption before it occurs?
2. What are the perceived elements or lack of elements that get in the way of dealing with disruptions successfully?
3. What are the perceived reasons for the internal auditor's participation in the development and implementation of business continuity planning?
4. What are the perceived reasons for not involving the internal auditor in business continuity planning?
5. Overall, how could government agencies mitigate the impact of a disaster without the input of the internal auditor?
6. What can mitigate the impact of the service disruptions other than the use of business continuity planning?
7. What are the roles of the internal auditor in enterprise risk management within the government sector?
8. How does enterprise risk management relate or defer from business continuity planning?
9. What steps considered in the development and implementation of business continuity planning? Can any of the steps be completed without the input of the internal auditor?
10. How should the internal auditor be involved in business continuity planning within in the government sector?



11. If the internal auditor should be involved in business continuity planning, what are the areas they could be excluded (e.g., business impact analysis, security risk assessment, recovery strategy, disaster recovery plan, update/maintenance) and why?
12. How should the internal auditor be involved in business continuity planning in the government sector?
13. What could be the reaction of those charged with governance regarding internal auditor's roles in business continuity planning?
14. If the internal auditor participates in the business continuity planning, what are the necessary safeguards to mitigate the impairment of independence?
15. If the internal auditor does not participate in business continuity planning, what are risks to the government sector, if any?